Warfighter IT Interoperability Standards Study

Final Report

July 22, 2012

Prepared for:
Office of the Army Chief Information Officer
Architecture, Operations, Networks and Space Directorate
Information Architecture Division
Arlington VA 22202

and

CECOM Life Cycle Management Command
Software Engineering Center (SEC)
Army Net-Centric Data Strategy Center of Excellence (ANCDS CoE)
Aberdeen MD, 21005

Prepared by:
Richard Bleach, PhD, Principal Investigator
Peter Morosoff
Jeff Seeley

E-MAPS Inc.
Email: e-maps@e-mapsys.com
Phone: 703-385-9320

and Booz Allen Hamilton

Task Order Subcontract Number:	98378XSB0P
Task Order Number:	002 (Revision)
Between:	Booz Allen Hamilton and E-MAPS
Prime Contract Number:	W15P7T-06-D-E401

UNCLASSIFIED

This page intentionally left blank.

Abstract

Creating interoperability requires that two or more people, organizations, or information technology (IT) systems use common semantic and format standards when communicating. For example, this abstract uses the grammatical format of sentences and paragraphs for a syntax standard and Webster's dictionary's terms and definitions as a semantic standard.

This report explains the findings and recommendations of the Warfighter Information Technology Interoperability Standards (WITIS) Study performed by Electronic Mapping Systems, Inc., (E-MAPS) for the Software Engineering Center, US Army Communications-Electronics Command (CECOM) on the standards available to facilitate interoperability across the IT systems developed to support Warfighters. Because many such standards are available to developers of such IT, the question is why interoperability problems persist among the Warfighter IT systems? What is missing? The study team found: first, there is no standard DoD definition of interoperability and, second, this leads to a variety of opinions by the managers and developers of IT as to whether interoperability is based on 1) just standards such as eXtensible Markup Language (XML) that address formatting but not semantics; 2) semantics (e.g., uniform understanding of the term fire support) and format (syntax); or 3) semantics and format plus relevant policy and procedures, registries, data architecture, and structures such as data models . The study team concluded that creating interoperability requires using the third set of elements (i.e., semantic, format [syntax], and policy and procedures). The biggest gap in creating semantic interoperability is insufficient Army and DoD policy and process on IT interoperability. Therefore, the study team recommends that, first and foremost, the IT interoperability gaps in Army and DOD policy and process be identified and closed. Additional actions should be taken to remedy shortcomings with registries and repositories, data architecture, and data models and ontology that impede IT interoperability.

This page intentionally left blank.

Table of Contents

Table of Figures

This page intentionally left blank.

Acknowledgements

The authors thank the following individuals for their support, advice, and information provided during this study: Mr. Cliff Daus (Army CIO/G-6), Mr. Jeff Maddox (Army CIO/G-6), Mr. Bruce Haberkamp (Army CIO/G-6), Mr. Lewis Saunders (Army CIO/G-6), Mr. Robert Landry (Army CIO/G-6), Ms. Yosira Martinez (Army SEC), Mr. Terry Edwards (Army ASA(ALT)), Mr. Philip Minor (Army ASA(ALT)), Mr. David Skidmore (Army PEO Missiles and Space), Mr. Larry Smith (Army PEO Missiles and Space), Mr. Charles Babers (Army PEO Missiles and Space), Mr. Claire Guthrie (Army PEO, IEW&S), Mr. Kevin Backe (Army Geospatial Center), Dr. Jens Pohl (Cal Poly Univ), LTC William Mandrick (Army 354th Civil Affairs Brigade), Mr. Anthony Petosa (Army RDECOM), Mr. Donald Porter (Army PEO C3T), Mr. Donald Makert (Research Innovations, Inc), Mr. Al Duncan (Army PEO EIS), Mr. Terry Wales (Army RDEC), Mr. Eric Byrd (Army PM Soldier Warrior), Mr. Ron Smetek (NGA NIAT), Mr. Bill Burkett (BAH), Ms. Mary Reddell (BAH), Ms. Shelley Bohlen (BAH), Mr. John Backert (BAH), and Ms. Jan O'Malley (BAH).

This page intentionally left blank.

Executive Summary

This study addresses how adoption of standards can help improve information technology (IT) interoperability that supports Warfighter operations in Army, Joint, Interagency and coalition missions. We used a broad definition of IT interoperability standards because past studies have shown that a variety of factors across the DOTMLPF spectrum contribute to IT interoperability. In this study, standards include standard policies and processes in addition to technical standards. There are variations in DoD definitions of interoperability. By IT interoperability we mean both 1) the exchange and 2) understanding of information exchanged that is then used to achieve operational effectiveness. This is the definition in Chairman of the Joint Chiefs Instruction (CJCSI) 6212.01F, "Net Ready Key Performance Parameter (NR KPP)." The IT systems considered in this study include both those that are used directly by Warfighters such as the Army Battle Command System (ABCS) and those that are supporting systems such as the General Fund Enterprise Business System (GFEBS).

There are several reasons for addressing how the adoption of standards can help improve IT interoperability. 1) Previous Army studies[1,2] have found that a lack of common terminology used by Warfighting IT systems hinders understanding of data and information exchanged. 2) Non-material factors, such as failure to establish common data and information exchanges based on standard doctrine and training impede the use of common terminology. 3) There is little that has been done to correct this shortfall. 4) Senior leadership and decision makers in the Army and OSD face increasing pressure to find and use more efficient ways to achieve capabilities such as IT interoperability among Service, Joint and coalition Warfighters. 5) Army and other DoD leadership have recognized that changes based on standards need to be made in order to create a more efficient way to use IT.[3] A 29 June 2012 memorandum entitled "DoD Data Framework", from the Deputy Assistant Secretary of Defense (C3 & Cyber), states that "Understanding the relationships of various data standards to one another is essential for developers, and the current data policy is insufficient for this purpose." The memo further states that "Some limited efforts by Communities of Interest (COI) facilitate information exchanges within a COI, but data understandability and interoperability beyond that COI is impaired because no rules or governance structure exists to enforce those elements among a more broadly based community."[4]

Based on the reasons above, results and recommendations from this study are intended to be considered and used by Army and other DoD leaders as alternative ways to achieve efficiency and effectiveness through better IT interoperability. The results of this study can also be used to assist DoD officials participating in development of the new DoD data framework requested in the 29 June memorandum.

To that end, *we strongly encourage the development and approval of policies and processes that 1) contain criteria which facilitate how users select and use appropriate IT interoperability standards and 2) specify metrics that can be used to evaluate how well those standards help achieve IT interoperability*.

Specifically, we recommend particular attention be paid to the following five categories of semantic standards, further described in section 4.2.3 of this report, in order to help improve the understanding of the information-exchanged aspect of IT interoperability.

- Vocabulary and terminology
- Data model and ontology
- Information architecture
- Repeatable process
- Authoritative data source and repository

Questions that may be useful in developing policies and processes that specify criteria for choosing semantic IT interoperability standards are contained in Recommendations (Section 5) of this report.

Although the study examined IT interoperability standards from both exchange and understanding perspectives, we found that there were far fewer standards on the semantics to be used to facilitate shared understanding among warfighters than there are standards on the formats to be used to exchange data and information among IT systems. This asymmetry of standards led us to focus on how to use standards for facilitating common understanding with data and information.

The study found that there are two key ways that a shared understanding of data and information is achieved when using IT systems. One way is by mediating existing IT schema, which can include mappings, translations, and other forms of reconciliation, to achieve agreement on the meaning of data and information with an emphasis on identifying synonyms in different IT schemas. A second way is by obtaining agreement on the meaning of data and information before it is inserted into IT schema. This second approach usually involves developing common vocabularies, lexicons, dictionaries, and ontologies upon which the schemas are then based. Although the study did not assess which approach is more efficient, evidence exists that the second approach has saved organizations time and effort in creating what we call data and information interoperability. *We recommend that a more thorough comparison be made of the efficiencies and effectiveness of approaches to achieving data and information commonality.*

One of the problems most encountered by developers of IT systems is how to locate and access appropriate standards for building and testing IT systems for interoperability. To address this issue, *we recommend that DoD policies and procedures be improved to clarify where standards are archived, can be accessed, and how they should be chosen and approved by authoritative bodies*.

The study was tasked to provide answers to questions previously asked by Army leadership in the CIO/G-6 and ASA(ALT) organizations concerning IT interoperability. These questions and answers are intended to help develop improvements to the Army IT policy and the Common Operating Environment (COE) Implementation Plan.

Although the terms data and information are often used inconsistently and generally understood to be distinct from each other, we did not distinguish between the two terms in addressing broad IT interoperability questions and issues.

The study found that one of the most effective ways DoD has implemented semantic interoperability is through use of the Joint Staff J-7's joint doctrine development system. This system includes: 1) the Joint Publications, 2) the Joint Doctrine, Education, and Training Electronic Information System (JDEIS), and 3) policy and processes published in Chairman of the Joint Chiefs of Staff instructions. With the help of this system, the Chairman of the Joint of Staff has been able to standardize the terminology of joint warfare across the Services and other DoD organizations. This has had a practical effect on Warfighter interoperability by establishing a standards-based semantic approach that facilitates operational interoperability and mission accomplishment. The Chairman of the Joint Chief of Staff's approach has important implications for DoD's efforts to achieve semantic interoperability among IT systems. These implications are: 1) publish policy and process in just two or three documents; 2) publish semantic standards in sources with the authority and thorough preparation of Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms;* 3) maintain one online primary authoritative data source registry / repository as the Joint Staff has done with JDEIS; and 4) designate appropriate authoritative body(ies).

The study questions and summarized answers are:

1. What is the current status of data interoperability standards (e.g., data models)? Standards are used in the two basic ways described above to achieving data and information commonality. Use-case analysis and a formal data call (see appendices C and D) confirmed that Army IT programs are achieving data and information commonality using a variety of standard data models (see Section 4.3.1) to help with either mediation or development of common vocabularies. Policy, process gaps, and issues associated with establishing data commonality standards have been identified from literature search, informal program manager contacts, and Warfighter interviews. These gaps and issues are described in this report.

2. How well do Army Warfighter systems comply with those standards? Communities of interest (COI) and IT systems' program offices surveyed comply with a variety of DoD and commercial standards for exchanging data and information. There are relatively few standards that are used to achieve data and information commonality, but IT systems that do use these types of standards generally use commercial standards from organizations such as the International Organization for Standardization (ISO) and American National Standards Institute (ANSI).

3. How well do the standards meet the interoperability needs of the warfighting area? Additional data commonality standards, in the form of policies, processes, and procedures, need to be developed and implemented to meet Warfighter needs according to Warfighter interviews and use-case and data-call analysis.

4. What are the steps in the process of establishing a set of interoperability standards? DoD policy, architecture, and governance directives and instructions specify the steps to review, coordinate, and approve IT interoperability standards at the DoD level through the CIO Executive Council and its subgroups. Steps to locate, access, and choose appropriate existing and emerging standards are mostly left up to designated authoritative bodies to determine.

5. What organizations are responsible for executing each step? At the DoD level, the DoD CIO has overall responsibility for the steps in a process of reviewing and approving proposed DoD IT interoperability standards. In the Army, the CIO/G-6 has overall responsibility for approving IT interoperability standards. The policy for review and approval of IT interoperability standards is contained in Army Regulation (AR) 25-1, "Army Knowledge Management and Information Technology." Other designated authoritative bodies such as the Army Data Board and communities of interest (COI) may select IT interoperability standards but there appears to be no overall process in the Army for doing so.

6. What information do they need to carry out each step, and where does that information come from? Currently there are no official criteria in the Army for choosing IT interoperability standards. The Army Information Architecture (AIA) contains sets of business rules and principles for exchange of data and information.

7. What alternatives to the recommended interoperability standards are already available? The recommendations from this study identify alternative potential standards in the form of criteria that may be used to set standard policies and processes for achieving both semantic and syntactic IT interoperability. However, shortfalls in policy and process remain. See the 29 Jun 2012 memorandum from the Deputy Assistant Secretary of Defense (C3 & Cyber).[4]

8. What is their level of maturity, and the cost and applicability? Alternative policy and process standards have yet to be developed, coordinated, and approved. At this time, use-case analysis has shown the potential for increases in efficiency to be realized but a business-case analysis needs to be performed to verify how much time, effort, and costs can be avoided.

Section 1 - Introduction

1.1 Background

In 2009, an Army study entitled "US and Coalition Forces (Data) Interoperability"[1] concluded that "there is a low level of semantic interoperability between major US and coalition C2 IT systems." Reasons for this condition included; 1) lack of standard procedures and formats for reporting event information, 2) lexicons not being developed that reflect doctrine, and 3) complex mechanisms for exchange of information.

A subsequent Army study in 2010 entitled "A Prototype to Deliver IT Interoperability"[2] identified key DOTMLPF factors that contribute to semantic IT interoperability and proposed a way to measure them. Recommendations from this study included incorporation of semantic interoperability metrics into relevant DoD processes such as certification, accreditation, and testing of IT interoperability.

In September 2010, Assistant Secretary of the Army (Acquisition, Logistics, and Technology) (ASA[ALT]) leadership asked several questions relating to semantic interoperability that could provide answers to help plan for the evolutionary acquisition of Army IT systems.

The questions were:

- What is the current state of data models with respect to being able to represent the functional areas of interest to the Army such as logistics, maneuver control, and intelligence?
- Why is the adoption of data models critical to IT systems that are used for information sharing in a net-centric environment?
- What is the state of existing systems in terms of compliance with current data models?
- What is a practical roadmap that can guide the evolution of existing and future IT systems to use of common data models in a net-centric environment?

In October 2010, the Army CIO/G-6 and ASA(ALT) leadership co-signed a joint memorandum that linked an Army Common Operating Environment (COE) architecture with an effort to plan for implementing that architecture. The memo states "The COE Architecture and Implementation Plan will provide direction to our industry partners regarding our framework standards." The computing environments that are part of the COE are now in the process of determining which standards are most appropriate to use to achieve IT interoperability.

The objectives for this study were formulated, in part, to help answer the ASA(ALT) questions listed above and to assist in developing plans for achieving IT interoperability with the Army Common Operating Environment (COE).

1.2 Assumptions

It is assumed that the definition of IT interoperability found in Chairman Joint Chiefs of Staff Instruction (CJCSI) 6212.01F, "Net Ready Key Performance Parameter (NR KPP)," which includes "operational effectiveness of that exchanged information as required for mission accomplishment" means that in order to achieve IT interoperability, semantic understanding of data and information is needed in addition to exchange of that data and information between machines.

It is assumed that the use cases and the data call analyzed in this study are representative samples of the entire COE set of programs.

It is assumed that study results for Warfighting IT systems may also be applicable to supporting IT systems such as business systems.

1.3 Document Overview

This report consists of six sections and four appendices.

Section 1 (page 7) provides introductory explanations of why and how the study came into being, and what assumptions were made to base our analysis and recommendations on.

Section 2 (page 11) states the purpose of the study, the six tasks that comprise the study effort, and the primary objectives of the study.

Section 3 (page 12) describes how the six study tasks were accomplished, the methodology used to analyze results, and the questions the study was asked to answer.

Section 4 (page 15) presents the results of analysis of 1) gaps, overlaps, and issues 2) existing and emerging standards, and 3) alternatives for using Warfighter interoperability standards that were identified in literature searches, use cases and the data call to the six Army Common Operating Environment (COE) computing environments (CEs). Answers to the study questions identified in Section 3.2 are given on Section 4.3.2.3 of this section.

Section 5 (page 45) gives recommendations to Army and DoD stakeholders on actions that can be taken to improve Warfighter IT interoperability.

Section 6 (page 51) describes overall conclusions made as a result of this study.

Appendix A (page 55) is a list of references.

Appendix B (page 59) is a glossary.

Appendix C (page 75) is a summary spreadsheet containing pros and cons for standards analyzed in this study.

Appendix D (page 80) is a summary of responses from the data call.

This page intentionally left blank.

Section 2 - Purpose, Scope, and Objectives

2.1 Purpose

The purpose of this study is to analyze, report on, recommend, and present to stakeholders how the Army and the DoD can make IT interoperability more efficient and effective by adoption of standards.

By interoperability, we mean the definition given in the CJCSI 6212.01F, Net Ready Key Performance Parameter (NR KPP) glossary which states that "*the ability to operate in synergy in the execution of assigned tasks. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/ or their users. The degree of interoperability should be defined when referring to specific. (JP 1-02) For IT (and NSS), interoperability is the ability of systems, units or forces to provide data, information, materiel and services to and accept the same from other systems, units or forces and to use the data, information, materiel and services so exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the operational effectiveness of that exchanged information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the lifecycle and must be balanced with IA.*

In order to address the full definition of IT interoperability given in CJCSI 6212.01F, by standards we mean standard policies, processes, and procedures as well as the technical standards.

2.2 Scope

The scope of the study is described by the following six study tasks.

Task 1: Identify, analyze, and document existing standards for achieving IT interoperability among Joint/Interagency/Multinational (JIM) information systems, including those for information exchange and understanding. A data call to programs of record based on Army CIO/G-6 priorities will be used to help collect this information.

Task 2: Identify and document gaps, overlaps, and issues with the current Army Common Operating Environment (COE) plans for using and evolving these standards to achieve improved Army enterprise IT interoperability among warfighter system capability sets.

Task 3: Identify and document emerging and mandated DoD standards and external standards that are aimed at achieving IT interoperability among JIM forces.

Task 4: Analyze and document alternatives for improved warfighter IT interoperability standards, including pros, cons, and priorities.

Task 5: Recommend enterprise standards across the DOTMLPF spectrum that can be used for both exchange and understanding of information shared, including standard processes, that the Army can use to plan for the achievement of efficient and effective IT interoperability utilizing warfighter IT systems.

Task 6: Identify and document actions that can be taken by registries and repositories holding standards and related documents to facilitate the use of these registries and repositories and the information they hold.

2.3 Objectives

The study has two primary objectives.

Objective 1: Conduct analyses of IT interoperability standards and repeatable processes to determine how best the Army can adopt standards and standard ways of using IT in order to improve the efficiency and effectiveness of the Joint/Interagency/Multinational information sharing environment.

Objective 2: Develop and present recommendations that enable US Army architects, system developers, and system testers to plan and implement common enterprise IT interoperability standards, including standard processes, in programs of record (PORs), systems of systems, and families of systems. Present and explain recommendations to study stakeholders.

Section 3 - Study Approach

3.1 Tasks and Methodology

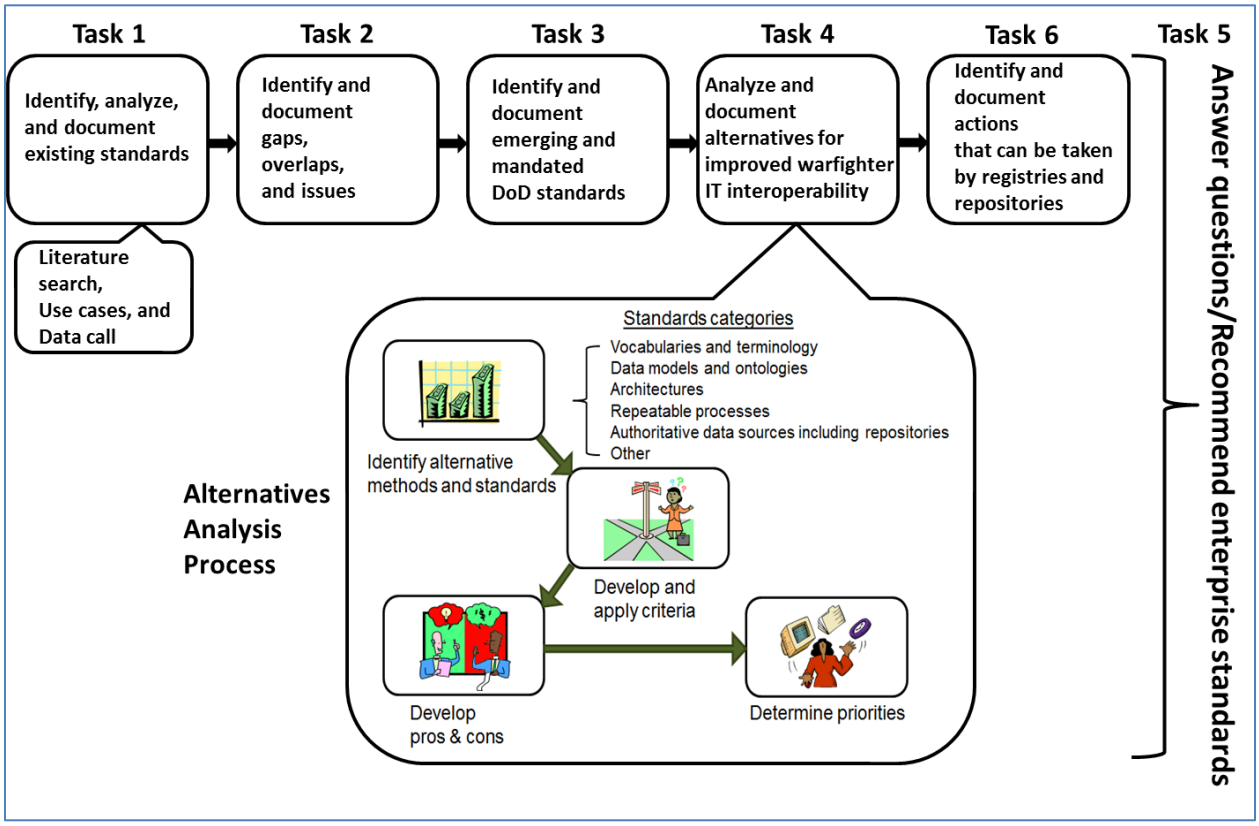

Figure 1 - Study Tasks and Methodology

Figure 1 shows the approach used to perform this study. It consists of six tasks that progressively accomplished activities specified in the study performance work statement.

Task 1 focused on identifying the existing standards that guide the development and use of Army IT systems for interoperability purposes. It was accomplished with the help of a literature search, several use cases, and a data call to Army IT programs that support Warfighter missions.

Task 2 identified major gaps and issues associated with achieving IT interoperability from both developer and Warfighter perspectives. It involved analysis of use case documents, data calls information, and discussions with developers and Warfighters.

Task 3 identified emerging policies, processes, and data models that have the potential to be used as standards both now and in the future.

Task 4 developed a methodology that could be used to help evaluate alternative standards for use in achieving semantic IT interoperability. The methodology includes candidate criteria to determine the pros and cons of choosing specific IT standards and assessing priorities in choosing and implementing those standards.

Task 5 provided initial answers to questions asked of the study team. These are listed below and include recommendations.

Task 6 identified actions that can help facilitate the use of authoritative data in IT registries and repositories in order to improve IT interoperability.

3.2 Study Questions

The questions addressed by this study are, in part, questions from the Director, System of System Engineering (SOSE), Assistant Secretary of the Army (Acquisition, Logistics, and Technology (ASA[ALT]) (see page 7) and the Army CIO/G-6 AOD organization. The study questions are:

- What is the current status of data interoperability standards (e.g., data models)?
- How well do Army Warfighter systems comply with those standards?
- How well do the standards meet the interoperability needs of the warfighting area?
- What are the steps in the process of establishing a set of interoperability standards?
- What organizations are responsible for executing each step?
- What information do they need to carry out each step, and where does that information come from?
- What alternatives to the recommended interoperability standards are already available?
- What is their level of maturity, and the cost and applicability?

Answers to these questions are found in Section 4.4.

Section 4 - Analysis of IT Interoperability Standards

4.1 Gaps, Overlaps, and Issues

There exist gaps and issues with implementing IT standards for interoperability. There is a plethora of IT standards in existence today that are found in multiple places with overlapping purposes. This can present a significant challenge for program managers and PEOs who must select the standards that will make their IT systems interoperable. Analysis of existing Army and DoD architectural and policy guidance has identified the following overarching gaps.

Gap 1: There is no single standard process to help Army program managers choose IT interoperability standards. The poor semantic interoperability among Warfighter IT systems may have been caused, in part, by the urgency that was placed on sharing information in overseas contingency operations. Systems such as Command Post of the Future (CPOF) were fielded relatively quickly because Warfighters could not understand how to achieve the semantic interoperability they needed with program of record (POR) IT systems. This lack of semantic interoperability among POR IT systems seems to have been largely the result of an absence of a single standard process to facilitate cooperation across the PORs while those systems were being developed. Additional IT systems, such as Combined Information Data Network Exchange (CIDNE), were developed quickly and with their own vocabularies and added to the collection of IT systems being used in theaters of operations. Semantic interoperability among CPOF and other IT systems was provided mainly 1) after initial fielding by 2) using semantic translation and mapping techniques. Again, the lack of a single standard process appears to have impeded developers building in cross-system semantic interoperability.

Therefore, Gap 2: There is a lack of attention to ways to use semantic standards to promote efficiencies and effectiveness in IT. As a result of the factors just discussed, a complicated collection of complex networks, IT systems, vocabularies, and information flows has arisen to enable the interoperability Warfighters need. This, in turn, has led to many IT systems and their associated data bases not being used as effectively and efficiently as possible.[1, 2] As an example, the Unmanned Aircraft Initiative found that "The initial assessment is that the greatest interoperability enhancement would result from conformance and enforcement of standardized data/metadata formats (sensor and platform generated data) so all UAS data is archive-able, searchable, retrievable and distributable by, and to, a wide range of (appropriate) users. Standardizing data output will significantly lower acquisition and development costs of ALL downstream users of that data extending into the Joint, Interagency, Intergovernmental and Multi-national (JIIM) domains."[5]

Two corollary issues to the above gaps can be identified as well.

> Issue 1a: There is no standard process being used by the Army to measure the level of IT interoperability for the purpose of assessing the value of IT in supporting interoperability.

Issue 2a: It is difficult to locate standards for establishing semantic interoperability in existing IT repositories.

It is important to note that effective IT interoperability requires data exchange that comply precisely with both semantic and syntax standards. An extra space or a wrong letter can make it impossible for an IT service to respond to data presented to it for processing. Users of telephones and those with email experience understand the need for such precision because of the results of a single wrong digit when making a telephone call or a single wrong character when entering an email address. This requires that standards be detailed, clearly written, and explain what they relate to (e.g., all weather data, all locations, requisitioning supplies, or fire support).

4.2 Existing and Emerging Standards

This section describes the distinction between semantic and syntactic standards, existing DoD policy and guidance related to IT interoperability standards, and semantic standards in functional groupings.

4.2.1 Semantic and Syntactic Standards

In our research we found that IT interoperability standards can be grouped into two categories; semantic and syntactic standards. This is illustrated in figure 2.

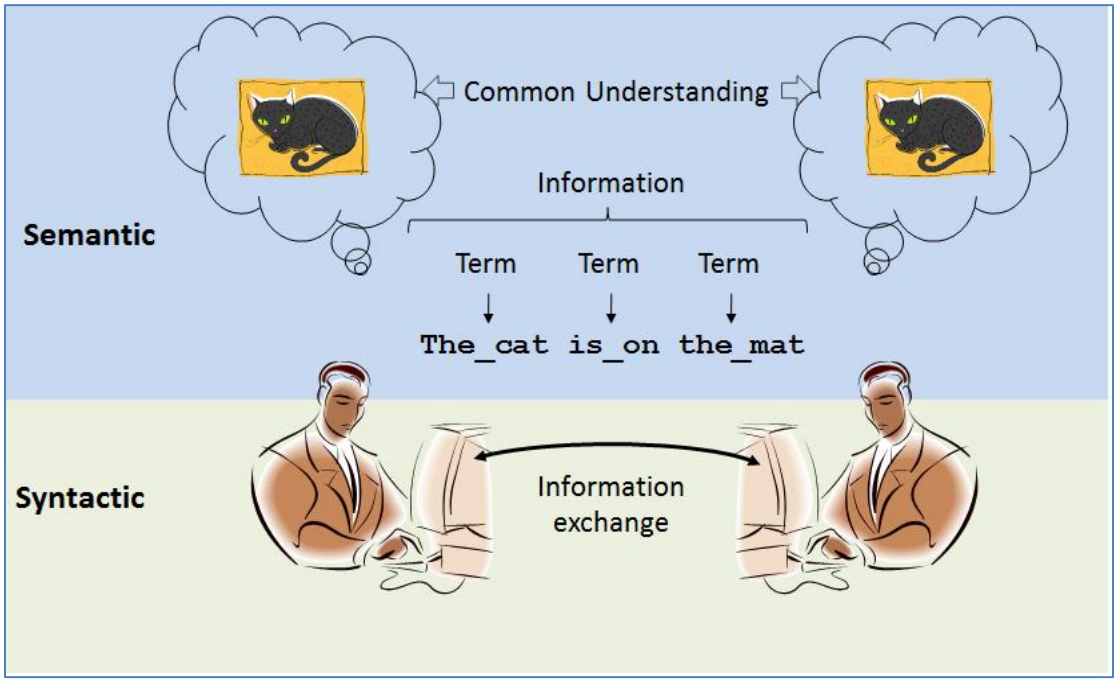

Figure 2 - Semantic and Syntactic Parts of IT Interoperability

By semantic standards we mean those standards that 1) identify the terms and meaning of the terms of which shared data are composed, 2) organize the terms with relationships among the terms, and 3) provide policy and process for creating authoritative sets of terms (e.g., vocabularies). Examples of this type of standard are the Joint Publications, which provide the terminology of joint warfare, and the Global Force Management Data Initiative (GFM-DI), which provides unique identifiers for, among other things, organizations and people. Semantic standards also include policy- and process-type guidance for creating vocabularies that are subsequently designated standards and used to ensure semantic interoperability. Examples are International Organization for Standardization (ISO) 1087, "Terminology Work -- Vocabulary -- Part 1: Theory and Application," and ISO 704, "Terminology Work -- Principles and Methods".

The study found that standards related to the semantics of data and information are less well documented and studied than syntactic standards.

By syntactic standards we mean those standards that are used to support the exchange of data and information among IT systems by standardizing format of exchanges. Examples of this type of standard are the Resource Description Framework (RDF) and Extensible Stylesheet Language Transformations (XSLT). Standards related to the exchange of data and information have been well documented and studied. DoD registries such as the DoD Information Technology Standards Registry (DISR) contain many of these standards. Other organizations such the International Organization for Standardization (ISO), Institute of Electrical and Electronics Engineers (IEEE), and the American National Standards Institute (ANSI) have published standards that are used by both government and commercial enterprises to facilitate creating IT interoperability. Warfighters have long used syntactic standards for information sharing (e.g., the call for fire format and the format for requisitioning supplies)

Some standards can be considered to be both semantic and syntactic standards. For example, schemas for exchange based on syntactic standards may be developed and used to help reconcile the meaning of data based on semantic standards. This concurrency can lead to confusion as to how semantics are addressed. This study attempts to clarify this issue by showing that there are at least two ways to address data commonality and associated standards in use today by Army PORs.

This study focused on data and information semantic standards because of the relatively few semantic standards from which authoritative bodies can choose.

4.2.2 Policy and Guidance Standards

4.2.2.1 OSD and Joint Staff Policy and Other Guidance Related to Semantic Standards

The "DoD Net-Centric Data Strategy" that was issued in May 2003[6] includes the goals of making data 1) understandable through COI-specific ontologies and 2) interoperable by, among other means, creating metadata.

DoD policy on information sharing in draft DoD Directive 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the DoD," states that:

> 1) "Data, information, and IT services shall be considered understandable when these assets can be consumed (e.g., structurally and semantically) by the intended and unintended users and when it can be readily determined how those assets may be used for specific needs. Data assets shall have associated semantic and structural metadata (vocabularies, taxonomies, and ontologies) published in the federated DoD Metadata Registry (MDR)."
>
> 2) "Data, information, and IT services interoperability shall be supported by making data assets understandable and enabling business and mission processes to be reused in compliance with established technical, data, and services standards and in accordance with 'DoD Chief Information Officer Memorandum, "Department of Defense Information Enterprise Architecture,' Version 1.2, May 7, 2010."

DoD Directive 8320.02 also states that data, information, and IT services shall be managed through governance structures (e.g., COIs, portfolios) and acquisition concepts, programs of record and initiatives that integrate metadata standards, processes, registries, security (including data aggregation), and common (shared) vocabularies[7]. Specific guidance includes:

> "DoD concepts, programs, projects and initiatives shall implement net-centric (e.g. Universal Core (UCore), National Information Exchange Model (NIEM)) and tactical (e.g. Variable message format (VMF), tactical data links (TDLs)) information exchange standards where applicable".

The DoD Information Enterprise Architecture (IEA) version 1.2 contains the following data services deployment business rules pertaining to semantic interoperability[8].

> i. All authoritative data assets and capabilities shall be advertised in a manner that enables them to be searchable from an enterprise discovery solution.
>
> ii. Data will be described in accordance with the enterprise standard for discovery metadata (the DoD Discovery Metadata Specification (DDMS)).
>
> iii. COIs should develop semantic vocabularies, taxonomies, and ontologies.
>
> iv. Semantic vocabularies shall re-use elements of the DoD Intelligence Community (IC)-Universal Core information exchange schema.
>
> v. Vocabularies, taxonomies, and ontologies must be registered with the enterprise for visibility, re-use and understandability.

The CJCSI 6212.01F contains the following guidance for measuring the effectiveness of information exchanged for interoperability purposes.

> "For each information element, Measures of Performance (MOP) are used to measure the information element's production or consumption effectiveness. Net Ready Key Performance Parameter MOPs should describe how the information elements will support unanticipated uses as described by the DOD Data and Services Strategy criteria of visible, accessible, usable, trusted, and interoperable."

4.2.2.2 Secretary of the Army Policy and Guidance Related to Semantic Standards

On September 9, 2011, the Secretary of the Army issued a memorandum on information technology management reforms that directed the Army Chief Information Officer (C IO/G-6) "to develop a comprehensive proposal to modernize the Army's network while realizing enterprise-wide efficiencies, with a target to achieve $1.5B in overall savings per year by the end of Fiscal Year 2015. " This memo cited the following issues with the Army's information technology network.

> "Current organizational and business process barriers prevent us from leveraging current technological innovations and impede success"
>
> a. "IT governance is complex, duplicative and overlapping, and the current IT modernization process is neither agile nor responsive."
>
> b. There is "excess network operations capabilities and overlap in our Command and Control, Tactical and Intelligence systems and within supporting networks."
>
> c. "The Army-wide IT workforce is out of balance and requires re-alignment."

To address the above issues, the Secretary of the Army has requested that options be proposed for the following areas:

> a. "Streamline IT governance and portfolio management functions in Headquarters, Department of the Army by clearly defining the discrete roles, responsibilities and authorities of key stakeholders."
>
> b. "Establish technical standards for the network infrastructure, applications and C2 systems software that maximize compatibility throughout the network, and baseline IT service standards for general support services. Any new approach identified must ensure visibility and accountability of all IT expenditures throughout the Army."
>
> c. "Consolidate, update, modify or eliminate outdated, redundant or unnecessary IT policies, organizations, activities and processes. Provide recommendations to balance the IT workforce across the Army."
>
> d. "Develop a plan that would propose an agile acquisition process consistent with the Common Operating Environment that addresses IT requirements identification, validation, testing and research and development."

4.2.2.3 Army CIO/G-6 Guidance Related to Semantic Standards

At her town hall meeting on Nov. 9, 2011, LTG Lawrence, Army CIO/G-6, presented guidance[9] stating that "*The network….has to be a single, secure, standards-based environment that ensures access at the point of need and enables global collaboration"*

AR 25–1, paragraph 4–8, identifies four Army data standards vital to implementing the data goals: authoritative data sources (ADS), enterprise identifiers (EID), information exchange standard specifications (IESS) and eXtensible markup language (XML). An ADS is a data asset designated as authoritative by an authoritative body (AB). An EID is an implementation of an independent identifier for a real or abstract asset. IESS is a standardized specification of a data asset that is exchanged. XML is a tagging language that provides a format to describe and annotate data being exchanged.

In addition Department of the Army Pamphlet (DAPAM) 25-1-1, "Information Technology Support and Services," specifies:

> "Architecture development standards are needed because the semantic meaning and rules for information exchange need to be determined. It is important to remember that XML does not create semantics; it uses already created semantics. Semantics need to be captured and documented in the integrated architecture development process and products. In the context of data interoperability it is vital to focus on data-related architecture products and model those elements that help develop the COI and cross-COI Ontology. Data-centered ontologies include entities, relationships, properties, values, and axioms/rules"

The Army Information Architecture (AIA) version 4.0 provides guidance for semantic interoperability through its data principles and business rules. For example:

> Business Rule DSD-22a: COIs shall create and maintain a DODAF AV-2 Integrated Dictionary and should create and maintain a DIV-2 Logical Data Model.

The AV-2 documents the "common vocabulary" of a COI and the DIV-2 documents the abstract, logical view of the data exchanged among members of the COI.

Army CIO/G-6 document "LandWarNet Powering America's Army[10]" states that "For the Network to be reliable and trusted, the Army must tighten IT governance and policies… to eliminate the plethora of publications, from memoranda to formal policies to interim updates, that govern information technology. The Army cannot reasonably expect its commanders to operate and maintain the Network properly without a definitive playbook. *The CIO/G-6 therefore intends to consolidate to just two authoritative sources: Army Regulation 25-1 and Army Regulation 25-2*. To ensure that these documents reflect the current state of technology and Army TTPs, they will be updated annually."

4.2.3 Semantic Standards in Functional Groupings

The topic of semantic IT interoperability has been discussed many times in the literature. Categories of research and case studies for addressing standards associated with the semantic part of IT interoperability are:

1) Vocabularies and terminologies
2) Data models and ontologies
3) Information Architectures
4) Repeatable processes relating to development, testing, operation, and governance of IT systems
5) Authoritative data sources and repositories

Existing and emerging standards for each of these categories and the basis for calling them standards are described below. Collectively, these five categories form a semantic interoperability model.

4.2.3.1 Standards for Vocabularies and Terminology

Many of the vocabulary and terminology standards in use today are associated with sharing of data over the World Wide Web. For example, Web Ontology Language (OWL) is a standard suite of knowledge representation languages that are used to develop ontologies. These languages are based on Resource Description Framework (RDF) and Extensible Markup Language (XML) formats. OWL is built on a set of standards developed by the World Wide Web Consortium (W3C), which is composed of member organizations, paid staff, and interested members of the public.

There are several ways in which IT standards are established. The ANSI has an ad hoc group that deals with ontology standards. The World Wide Web Consortium (W3C) establishes ontology standards such as OWL. Other standards-setting organizations include the International Organization for Standardization (ISO) and the Federal Geographic Data Committee (FGDC).

Vocabularies for several domains exist as de facto standards within a given domain. For example, the "Weapons Technical Intelligence Improvised Explosive Device Lexicon[11]" , developed jointly by the Defense Intelligence Agency (DIA) and Joint Improvised Explosive Device Defeat Organization (JIEDDO) provides a vocabulary for use by people and IT systems involved in counter improvised explosive device (C-IED) operations. Partial use of this common vocabulary in IT systems such as CIDNE, CPOF, and TIGR has advanced the understandability and timeliness of information shared by Warfighters in Afghanistan.

Several communities of interest (COI) in the Army such as the geospatial, missiles and space and intelligence programs have also established standard common vocabularies for their domains. However, creation the subsets of those vocabularies that are needed

to create common terms and definitions that enable understanding across domains remains to be done.

4.2.3.2 Standards for Data Models and Ontologies

DoD guidance regarding data models is intended to establish net-centric capabilities using IT systems. This guidance includes:

> "DoD concepts, programs, projects and initiatives shall implement net-centric (e.g., Universal Core (UCore) and National Information Exchange Model (NIEM))".

In 2007, CIOs of the DoD and the Office of the Director for National Intelligence (ODNI) received recommendations from a task force investigating obstacles and enablers to information sharing between the defense and intelligence communities. The task force reported that:

> "One approach to mitigating this problem is to adopt existing agreements on semantics and syntax for concepts that are universal (or at least broadly common), thus forming a 'Universal Core' of implementable objects that will be used in information systems wherever practicable…[12]"

An interagency team was created to act upon the task force recommendations and by the end of 2007 Universal Core 1.0 was produced to deal with the when and where semantics of machine to machine information exchanges. Early adopters of UCORE included US Strategic Command (STRATCOM), US Joint Forces Command (JFCOM), National Security Agency (NSA), and the United Kingdom Ministry of Defense (UK MOD) to enable common semantic understanding of time and location information.

A next step was to deal with the what and who aspects of semantic understanding. The interagency team anticipated that UCORE2.0 would include these aspects, however, the team was asked to reach out to the Department of Homeland Security (DHS) and the Department of Justice (DOJ) and expand UCORE. What was discovered is that DHS and DOJ had been developing their own broad-based information-sharing model called the National Information Exchange Model (NIEM). NIEM was, by that time, being used by law enforcement and criminal justice organizations and included a logical entity exchange specifications feature. It was soon realized that UCORE and NIEM could complement each other, for example, by UCORE adding a who, what, where, when digest to NIEM messages so that the DoD could understand a NIEM conformant message coming from the DHS and DOJ communities. By 2008, UCORE version 2.0 had incorporated the who and what aspects of semantic information exchange and initiated pilots. Early UCORE pilot projects included those supporting the Joint Command, Control, and Consultation Information Exchange Data Model (JC3IEDM) and Maritime Information Exchange Model (MIEM).

By 2009, the DoD had created domain specific UCORE component models including C2 Core. In 2010 the DoD issued additional guidance for C2 Core maturation an implementation that included spiral development efforts and data pilots[13]. One pilot

sponsored by the Army CIO/G-6 demonstrated that semantic understandable exchanges between Warfighting IT systems and emulators could be accomplished using C2 Core.

Thus, the stage has been set for 1) the complementary models envisioned by the original task force and 2) a combination of UCORE and NIEM that will eventually become the standard data model at the framework level. In the DoD, meetings held in the fall of 2011 resulted in agreement to pursue this hybrid approach[14].

Even if a framework data model such as UCORE/NIEM were to exist, there is still much work to be done in developing domain specific component models such as C2 Core. Standard domain vocabularies have to be developed, terminology for interoperability agreed upon, and ontologies based on needed interoperability defined in order to form the basis for improved semantic interoperability. It appears as if much of this activity can be accomplished through a standard repeatable processes described below. Thus, there is a possibility to avoid large upfront costs for new information technology.

Semantic Web applications that can help automate and thus accelerate the development of ontologies are now commercially available from companies such as TopQuadrant in Alexandria, VA.

4.2.3.3 Standards for Information Architecture

The Federal Enterprise Architecture (FEA) is used as a management tool to facilitate aligning resources in order to improve business processes. It prescribes processes for creating and using enterprise architectures to obtain value for the enterprise. It also lists a logical information exchange matrix that details all the categories and classes of information exchanges.

The publication of the DoD Architectural Framework (DoDAF) 2.0[15] expanded the standard architecture views available in previous versions of the DoDAF to describe information. DoDAF 2.0 provides for conceptual, logical, and system views of information models that can be used to develop, test, and use the data and information intended to be exchanged among systems. Today, only a few IT programs of those reviewed in this study use the logical architecture view as a standard for these purposes. More often, IT programs use features of these architecture views, such as vocabularies and associated metadata, to show compliance with DoD requirements and acquisition policies. System views such as the System View (SV) 6 which specifies how syntax is used to exchange of data, seem to be the views most used for development and testing.

Army Regulation (AR) 25-1, *Army Knowledge Management and Information Technology*, establishes policies and assigns responsibilities for information management and information technology. It applies to information technology contained in both business systems and national security systems developed for or purchased by the Department of the Army. It addresses the management of information as an Army

resource, the technology supporting information requirements, the resources supporting information technology, and Army Knowledge Management as a means to achieve a knowledge-based force. Chapter 4 of AR 25-1 (December 4, 2008 version) contains detailed policy on the composition and use of architecture documentation within the Army. Sections 4.3 through 4.7 specify standard ways in which the Army architecture should be developed consistent with DoD IT architectures, standards and external architectures. Section 4-9 specifies that mission area and Domain leads, system owners, PEOs, and PMs will ensure their data architectures comply with Army and DOD data requirements by developing and maintaining data performance plan (DPP) artifacts in a DPP system (DPPS) environment wherein the standards, policies, procedures, data models, and business rules reside and are employed as appropriate.

The Army Information Architecture (AIA), developed by Army CIO/G-6, is derived from policy and guidance in 1) the DoD Information Enterprise Architecture (IEA) and 2) AR 25-1. The AIA contains standards and policies for both exchange and understanding of information. It is currently used mainly for assessing compliance with guidance and policy and not as a blueprint for developing IT. Figure 3 below, which was taken from the draft AIA version 4.0, illustrates the relationships among the AIA and other DoD and Army policy and guidance from the AIA perspective.

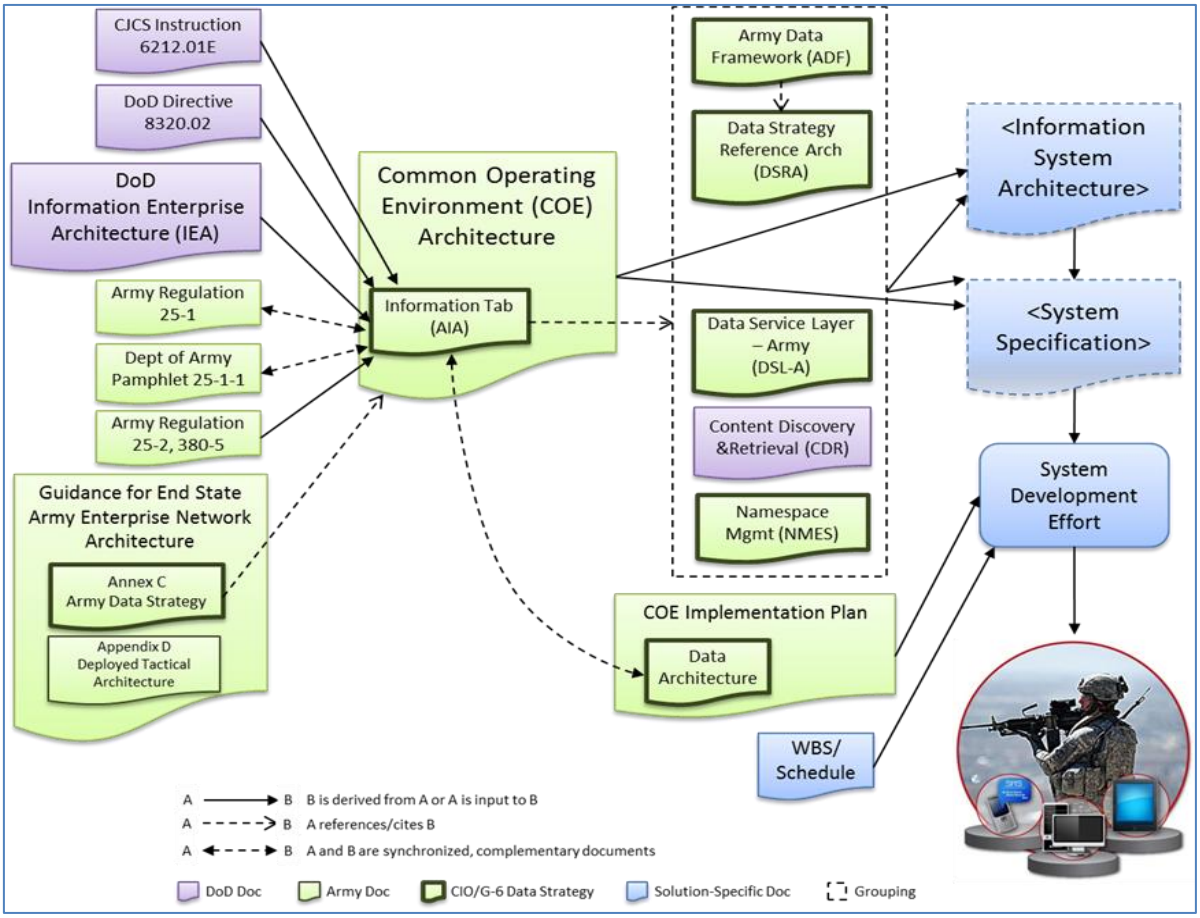

Figure 3 - Relationship of AIA to other DoD and Army Policy and Guidance

4.2.3.4 Standards for Repeatable Processes Relating to Development, Testing, Operation, and Governance of IT Systems

Repeatable processes are standards that can facilitate shortening development times as well as help ensure performance expectations are met. Because a repeatable process is usually a structured way of doing things, it facilitates unity of effort between efforts and organization and is more conducive to being automated than an ad hoc process.

Standard repeatable processes that can support IT interoperability have been proposed for achieving semantic understanding of shared information.

In OSD, the office of the Deputy Chief Management Officer (DCMO) has developed a repeatable process called Model, Data, Implement (MDI)[16], shown in Figure 4. It is based on modeling a business capability to be deployed, preparing and populating an information model and data store, and implementing capability by deploying business services. The goal is for these MDI processes to be automated so as to facilitate rapid development of architectures and business intelligence and rapid data management. The potential advantages include more effective and efficient IT interoperability.

The Military Decision Making Process (MDMP)[17] process already includes 1) the "modeling of the process" in the form of developing a plan and 2) "modeling the data" in form of determining the information/reports requirements. If the DCMO can develop an effective implementation of its MDI process, the process has the prospect to be extended to warfighter IT systems as well and used in conjunction with the MDMP or a process based on the MDMP.

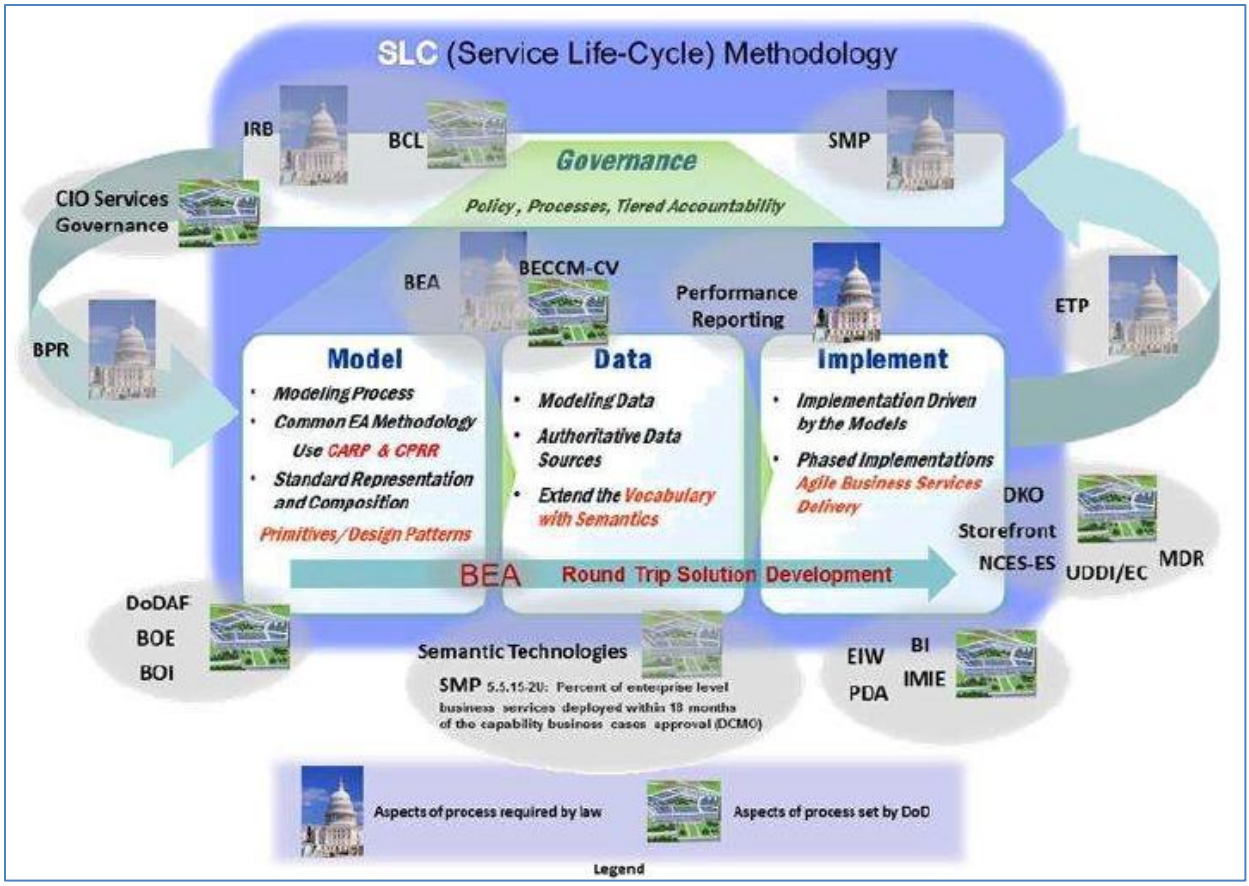

Figure 4 - Model Data Implement Methodology

There are a number of repeatable processes that have been developed which can be used to support standardization of semantic IT interoperability.

There exist examples of repeatable processes for creating ontologies. In areas suitable for Army program managers, there are methods that can be used to extend to a domain lexicon from a common upper ontology (CUO). The Basic Formal Ontology (BFO) and the UCore-Semantic layer (UCore-SL) are examples of Common Upper Ontologies.

A repeatable process for domain specific ontology creation[18] has been documented by LTC William Mandrick for use in creating Warfighter related ontologies. The process is broken down into five major activities:

1) Scope the domain,
2) Create initial lexicon,
3) Create initial ontology,
4) Verify and revise ontology, and
5) Publish ontology to potential users.

The process is intended to be a repeatable ontology modeling process that is designed to encapsulate ontology best practices and design patterns in order to improve the

quality of ontology development efforts and transfer ontology development knowledge and skills to a broader base of modelers.

Use of a domain specific repeatable process to implement an understandable exchange of key leader engagement (KLE) information across Warfighting IT systems has been demonstrated in a C2 Core Data Sharing Pilot. This process is shown in Figure 6.

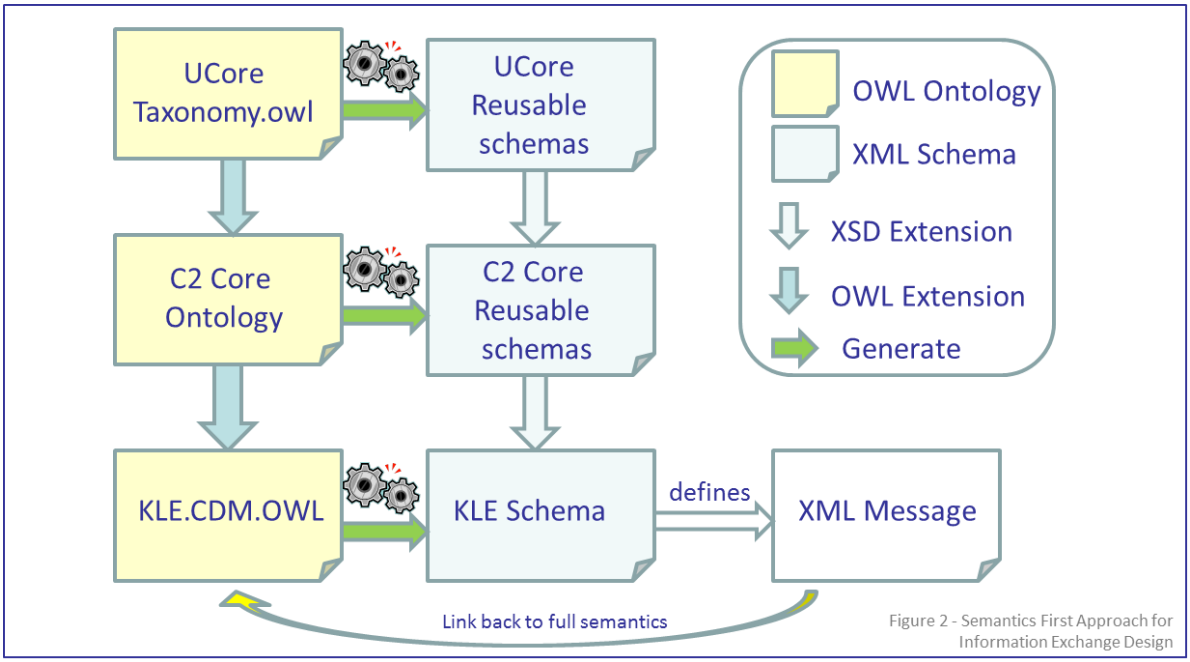

Figure 5 - Repeatable Process for Understandable Exchange of Information Used in C2 Core Pilot[19]

4.2.3.5 Standards for Authoritative Data Sources and Repositories

Joint Staff Instructions

CJCSI 8410.01 entitled "Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing" designates authoritative data sources that the Army will have to use because of that directive's requirement that the Warfighting Mission Area (WMA) IT portfolio invest only in IT products that are included in those repositories. WMA will use the authoritative DOD repositories listed below to data mine and choose recommended WMA portfolio IT investments for the portfolio. The authoritative data sources include:

(1) DoD Information Technology Portfolio Repository (DITPR). The DOD CIO developed DITPR as the DOD's official, unclassified portfolio management data source. All unclassified WMA IT and NSS investments to include unclassified component IT investments will be registered in DITPR. DITPR data extracts are imported into the Joint Information Technology Analysis and Management (JITAM) tool to support portfolio development.

(2) The DOD SIPRNET IT Registry. The registry is maintained by DOD CIO on the classified network and implements Title 40 direction to register all IT.

(3) Knowledge Management and Decision Support (KM/DS). The JROC's KM/DS is used by the JCIDS gatekeeper to record JCIDS documents and decisions, including the Joint Planning Document (JPD). It provides users with an electronic repository of guidance, issues, and results to facilitate decision making in the JROC process and enables users to submit documents and briefings, research topics, and request JROC/JCB for associated topics online, using a Web interface.

(4) DOD Data Warehouse. The Office of the Secretary of Defense, Director, Cost Assessment and Program Evaluation (OSD (D,CAPE)) DOD Data Warehouse contains 5-year Defense program and other programming and budgeting data collected by OSD(D,CAPE) as part of the PPBE process, to include integrated and embedded platform IT. To facilitate research, the DOD Data Warehouse is organized into data centers.

(5) Select and Native Programming Data Input System - Information Technology (SNaP-IT). SNaP-IT contains DOD IT financial information and generates reports mandated by the Office of Management and Budget and Congress for the DOD IT budget (reference q). It was developed and maintained by OSD (D,CAPE) as a web-based application used to collect nonstandard program and budget data requirements and is a DOD Data Warehouse feeder system.

(6) Joint C4I Program Assessment Tool-Empowered (JCPAT-E). JCPATE is an online tool and application suite used to assist OSD and the Joint Staff in accepting, staffing, reviewing, and evaluating Information Support Plans. Developed, maintained, and operated by the Defense Information Systems Agency (DISA), JCPAT-E provides the necessary electronic document distribution, comment collection and rollup, document storage, and management support necessary to evaluate draft documents. JCPAT-E is accessed on the classified network via https://jcpat.disa.smil.mil. It is accessed on the unclassified network via https://jcpat.disa.mil. JCPAT-E is also used to document IT investment interoperability certification information.

(7) System Tracking Program (STP). STP is the Joint Interoperability Test Command’s web database to track a system's progress toward joint or combined interoperability certification. The STP tracks complete NSS IT life cycle requirements document validation, testing, and culminates with certification status. It is located at http://stp.fhu.disa.smil.mil/.

Army Regulations

AR 25-1 specifies guidance and Army data standards management including authoritative data sources.

Section 4-9 specifies that data standards (specified in the DISR and other guidance documents) expressed as authoritative data sources (ADSs), information exchange standards specifications (IESSs), enterprise identifiers (EIDs), and eXtensible Markup Language (XML)) will be used to guide all data exchanges, including those needed to support legacy systems. Data management requirements will be included in IT planning documents.

Section 4-10 provides guidance on Authoritative Data Sources (ADS).

b. All Army organizations producing or using data standards (ADS, IESS, EID, XML) will

(1) Ensure that only Army-approved data standards are used in systems.
(2) Register new data standards in the appropriate part of the Data Performance Plan system (DPPS), as needed.
(3) Provide input to Army data standards reviews.

Data standards producers will use the Data Performance Plan System (DPPS). The DPPS is a centralized, metadata repository used for the procedural storing, universal viewing, and selective reuse of (all, or parts of) architectures, data models, business rules, and other DPP artifacts of functional Army systems. The DPPS content will be used to perform technical reviews of Army's functional data requirements. Information about Army data/metadata will be maintained and controlled in the DPPS as part of the standard metadata documentation.

Other authoritative data sources include:

- The Enterprise Authoritative Data Source Registry (EADS), which is intended to improve search, access, consistency and collaboration and consideration of services as well as to increase collaboration amongst producers and consumers.

- The DoD Architecture Registry System (DARS), which allows users to navigate the DoD Enterprise Architecture map to discover and access DoD Segment and Solution Architectures; and to create, view and edit architecture discovery metadata.

- The Army Capability Architecture Development and Integration Environment (CADIE), which offers a single, federated web-based environment for the development and discovery of integrated architectures across warfighting functions, and organizations throughout the Army Enterprise.

4.2.3.6 Example of Benefits of Implementing Standards in All Functional Areas

So far, this paragraph (paragraph 4.2.3) has discussed the following five groupings or areas of semantic standards individually: 1) vocabularies and terminology; and 2) data models and ontologies; 3) information architecture; 4) repeatable processes for

development, testing, operation, and governance; and 5) authoritative data sources and repositories. The paragraph now uses the joint doctrine development system to illustrate the value of these areas or groupings individually and collectively when seeking to create semantic interoperability.

The joint doctrine development system differs from the DoD development and acquisition programs in that the doctrine system is focused on providing warfighters and those who train them with joint publications which, among other things, facilitate semantic interoperability and more effective and efficient joint warfare. The acquisition and development activities that provide IT systems to warfighters are focused on providing IT systems. Some senior leaders and many others have hoped that the IT systems provided to warfighters would advance semantic interoperability, but this has not come to pass. The discussion that follows explains some of the reasons the joint doctrine development system has been so much more effective at creating semantic interoperability than the development and acquisition programs

The Director, Joint Force Development, Joint Staff (J-7), is responsible for the joint doctrine development system. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5120.02C, "Joint Doctrine Development System," states: "Use of joint doctrine standardizes terminology, training, relationships, responsibilities, and process among all U.S. forces to free JFCs (joint force commanders) and their staffs to focus their efforts on solving the strategic, operational, and tactical problems confronting them." Joint doctrine is in fact as well as policy the authoritative source of terminology that has led to semantic interoperability among warfighters in face-to-face discussions, in telephone calls, in email, in PowerPoint slides and in other communications.

The joint doctrine development system is effective at creating semantic interoperability because it is guided by 1) authoritative policy in the form of CJCSI 5120.02C, 2) authoritative processes published in Joint Chiefs of Staff Manual (CJCSM) 5120.02, "Joint Doctrine Development System," and 3) authoritative policy and processes for achieving semantic interoperability in CJCSI 5705.01D, "Standardization of Military and Associated Terminology." Consolidating the guidance on the joint doctrine development system into three issuances has had the practical effect and benefit that Lieutenant General (LTG) Lawrence is seeking through her plan to consolidate policy and process guidance bearing on LandWarNet into two documents. (See "LandWarNet: Powering America's Army" [http://ciog6.army.mil/LinkClick.aspx?fileticket=ONAWePgetXo%3d&tabid=36])

The joint doctrine development system is also effective because it has 1) an authoritative body, the Joint Doctrine Development Community (JDDC), 2) a chain of responsibility and authority that starts with the Chairman of the Joint Chiefs of Staff and flows through the Director, J-7, Joint Staff, to the JDDC, and 3) effective governance that implements the processes published in CJCSM 5120.02.

Additionally, the joint doctrine development system is also effective because it has a family of authoritative data sources to include 1) the Joint Doctrine, Education, and Training Electronic Information System (JDEIS), 2) the capstone joint publication, JP 1,

Doctrine for the Army Forces of the United States, 3) JP 1-02, *DoD Dictionary of Military and Associated Terms*, and 4) 80 other JPs that explain the terminology of warfare specialties (e.g., fire support).

The Joint Staff J-7's standardization of terminology is based on guidance in DoD Instruction 5025.12 that: "It is DoD policy: To improve communications and mutually understanding within the Department of Defense, with other Federal Agencies, and between the United States and international partners through standardization of military and associated terminology."

Members of DoD efforts seeking to implement semantic interoperability repeatedly told this study's principal investigator that their efforts were being impeded by 1) inconsistent policy and process guidance scattered over scores and possibly hundreds of authoritative documents, 2) difficult access on line to authoritative guidance and related information, and 3) lack of semantic standards. These issues were resolved for the joint doctrine development system long ago.

IT specialists who look at the joint doctrine development system often have difficulty seeing that system's versions of data models, ontologies, and information architectures. This is probably because IT specialists tend to think in terms of the formats that the IT community uses for data models, ontologies, and information architectures rather than in terms of the contents of such models, ontologies, and architectures. If one understands that an ontology is a formal representation of domain (as opposed to a document in the Web Ontology Language [OWL] format), then one realizes that each joint publication, with the exception of JP 1-02, is a formal and authoritative ontology for a particular domain (e.g., fire support) that includes models of data used in the JP's domain. For example, Section A, "Command Relationships" of Chapter IV, "Doctrine for Joint Command and Control," is a data model for command relationships formatted to make it as easy as possible for a person reading the JP 1 to understand the model.

Information architecture is defined on Wikipedia as "the art and science of organizing and labeling websites, intranets, online communities and software to support usability." IT specialist in and supporting DoD often expect an information architecture product be one of the standard views of the DoD Architecture Framework (DoDAF). This leads to many people looking at the JDEIS site (www.dtic.mil/doctrine) and not realizing that it is, the words of the Wikipedia site just quoted, a website organized to support usability of the JPs and other information.

The figure below is included because the study's principal investigator was told repeatedly that shortcomings in policy and process impede implementing semantic interoperability among the IT systems provided to warfighters. The figure below uses instructions and the joint publications to provide a model that the DoD's IT community should consider as it works through its policy and process challenges. The figure shows the flow of policy from the DoD instruction on standardizing military and associated to the Chairman of the Joint Chiefs of Staff instruction on this subject and then on to the implementation of this policy in the JPs. The figure includes the policy paragraph from

the DoD Instruction, the policy paragraph from Chairman of the Joint Chiefs of Staff Instruction, and a quotation form JP 1 on the role of doctrine in creating semantic interoperability. The figure also represents the existence of JP 1-02 and the other joint publications and their use to advance semantic interoperability.

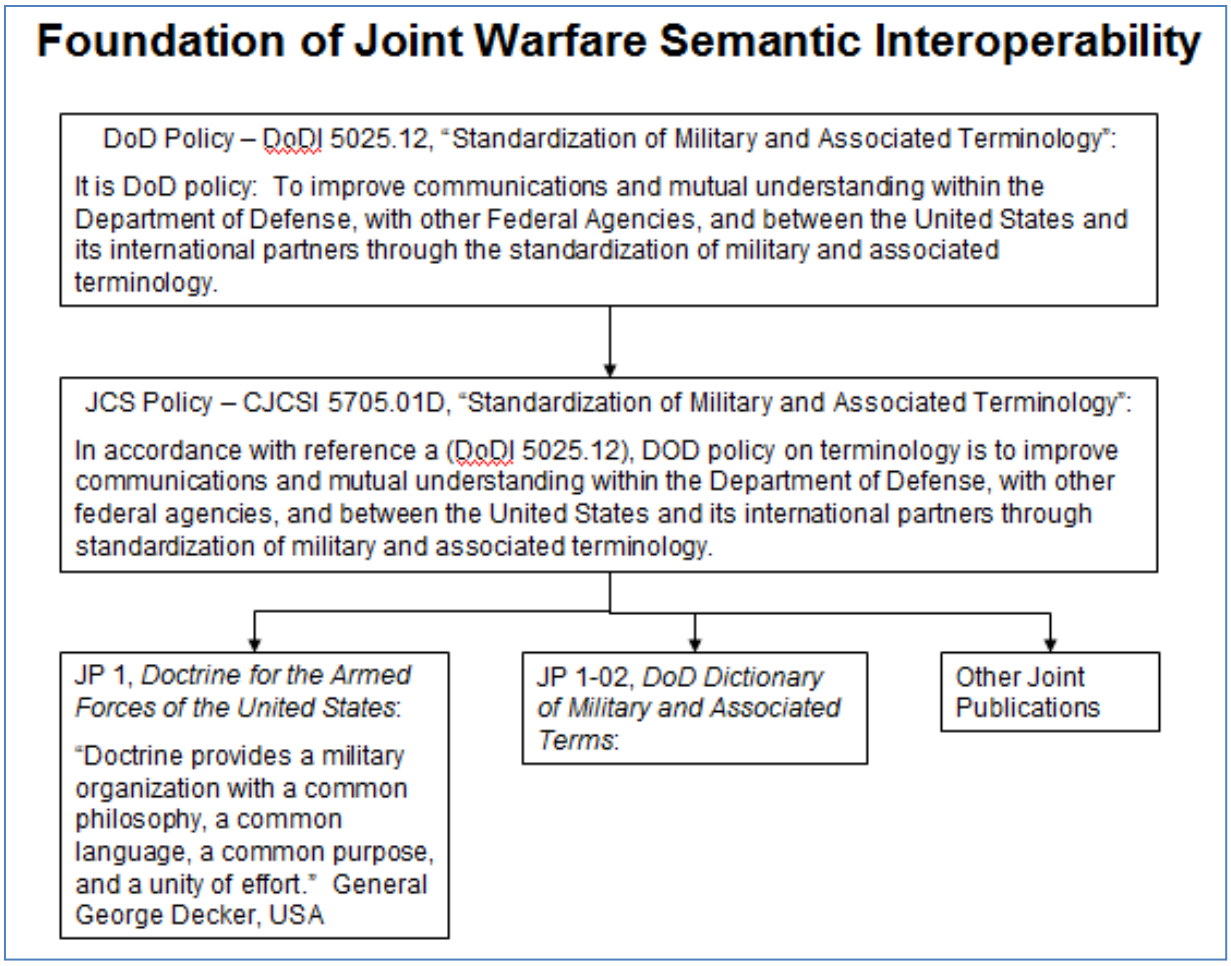

Figure 6 - Foundation of Joint Warfare Semantic Interoperability

4.3 Alternatives for Improved Warfighter IT Interoperability Standards

In today's budget constrained environment, it has become increasingly important for the Army and the DoD to look for ways to improve efficiency while maintaining the effectiveness of Warfighter support systems such as the IT systems that support interoperability among Warfighters.

The need to become more efficient across the DoD enterprise provides an opportunity to explore alternative ways of how standards, including those for semantic IT policy, processes, and technical specifications examined in this study, can contribute to making Army and DoD IT interoperability more efficient and effective.

Based on use-case and data-call analyses, this section describes alternative ways standard processes and data models are applied to help achieve Warfighting IT interoperability.

4.3.1 Use Case Alternatives

The following organizations provided information on alternative ways they use standards to develop IT systems that can help achieve Warfighting IT interoperability. This information was obtained from briefings, discussions, and participation in COE working groups. Each organization's input was considered as a use case.

- Joint Air and Missile Defense PEO
- Sensor computing environment working group (COE)
- Army PEO IEW&S
- Army Geospatial Center
- Army PM Battle Command
- National System for Geospatial Intelligence Interoperability Action Team

In addition, draft COE execution plans from the Sensor, Command Post, Data Center/Cloud, Mounted, Mobile Handheld, and Real Time/Safety computing environments (CE) were reviewed.

The findings from use case analysis are:

1) Data and information that have the same meaning among users in a domain is necessary to achieve IT interoperability as defined in DoD policy and legislation[20]. For this study, this condition is referred to as "data commonality".

2) There are two alternative approaches used today to create "data commonality:" a) creating common data prior to introducing it into IT system development and b) creating data mediation as part of IT system development.

3) Both the common data and mediated data approaches require human agreement on interpretation of data meanings. Each approach relies on different types of standards.

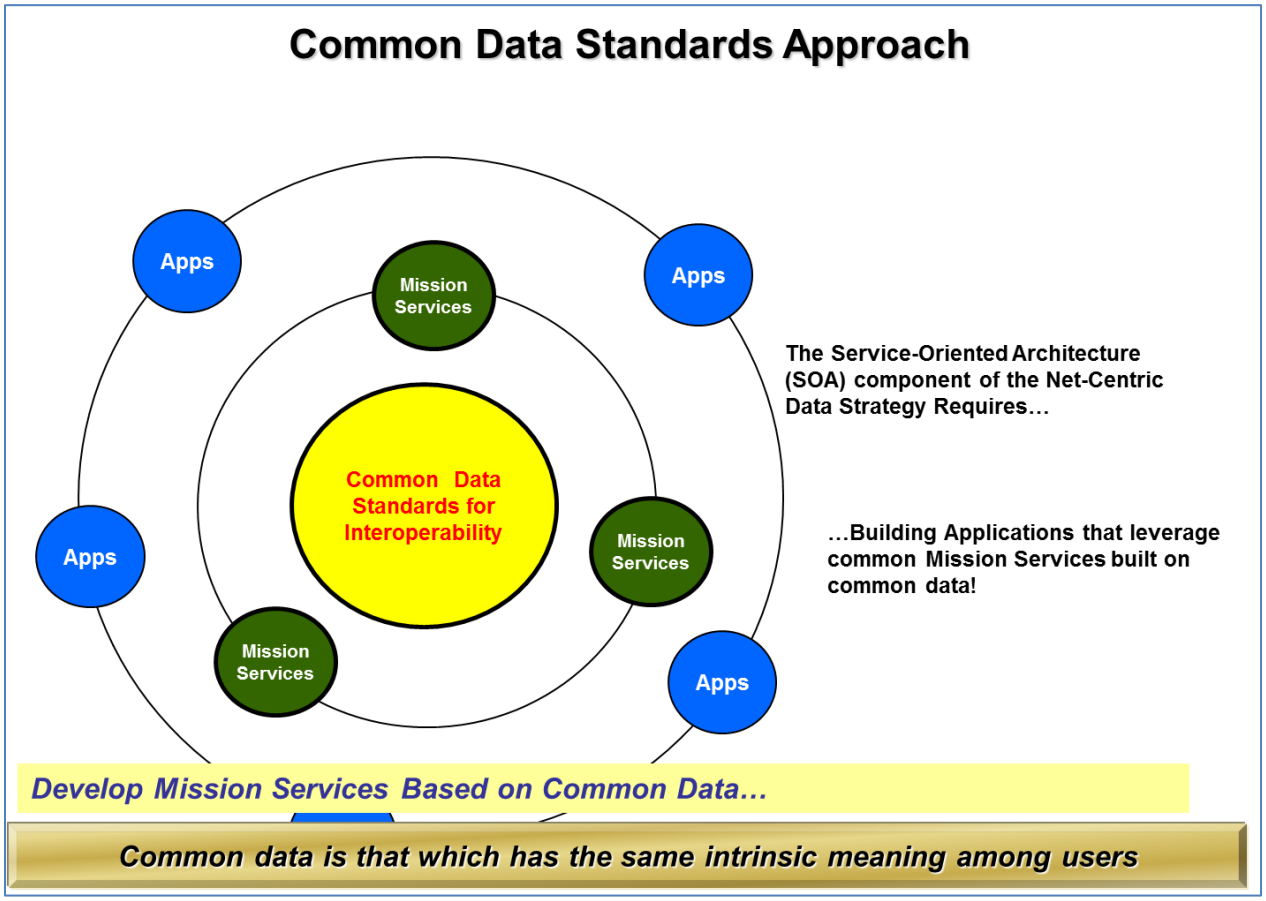

Figure 7 - Common Data Standards Approach

The common data approach shown in Figure 7 uses standards that apply to the creation and use of data so that data intrinsically has the same meaning among users.

The common data created by using these standards is then used to develop the schemas for exchange of data among IT systems.

An example of how this “common data” approach is being implemented by a program of record is shown in Figure 8.

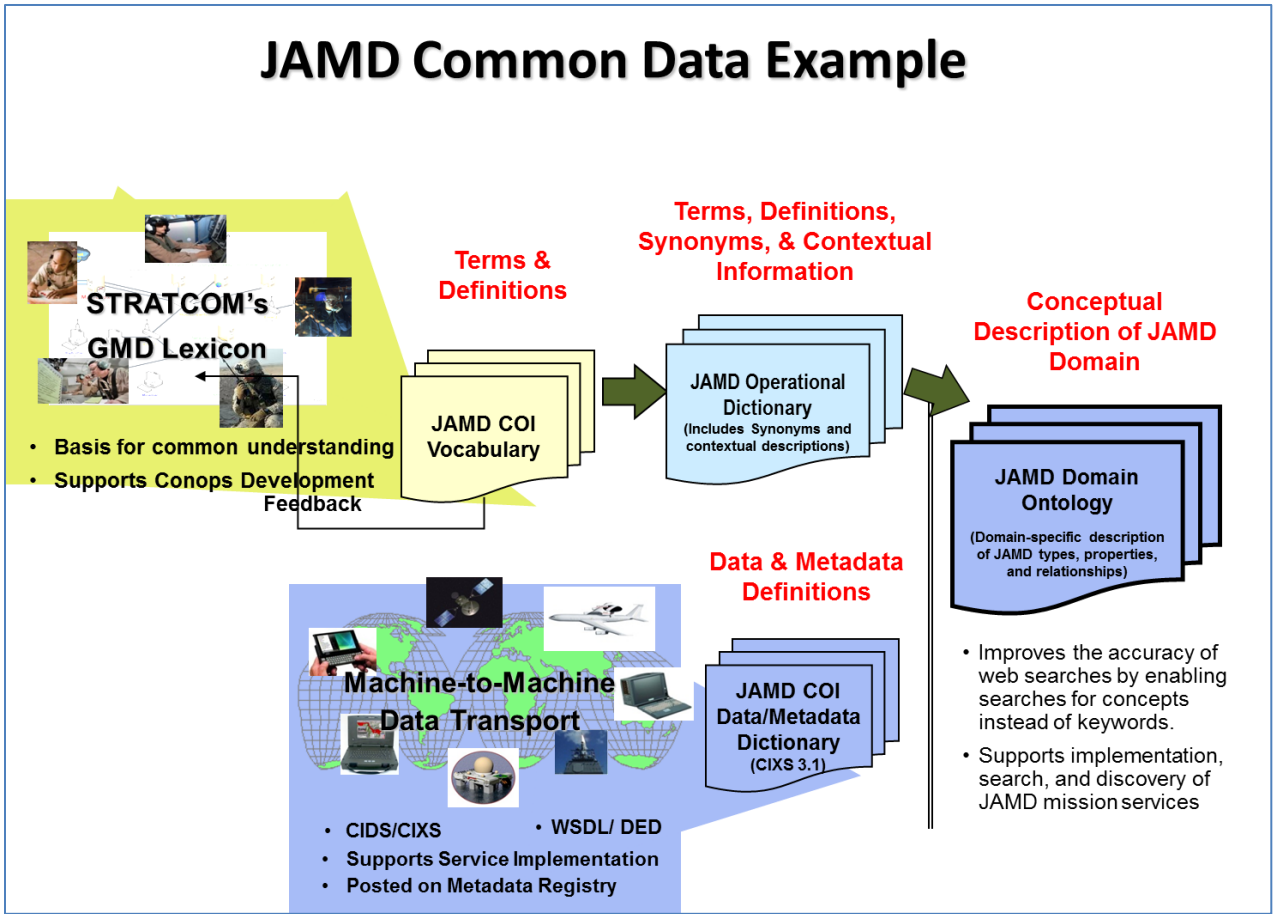

Figure 8 - Joint Air and Missiles Defense Common Data Process

The process used by the Joint Air and Missile Defense (JAMD) community is depicted in Figure 2. The process starts with a vocabulary based on an operational concept that is socialized within a Joint Community of Interest to obtain agreement on the meaning of terms in the vocabulary to be used. This vocabulary is documented in an operational dictionary and in a domain ontology which together help ensure that common semantics and relationships among terminology are reflected in IT exchange artifacts using the CIXS application.

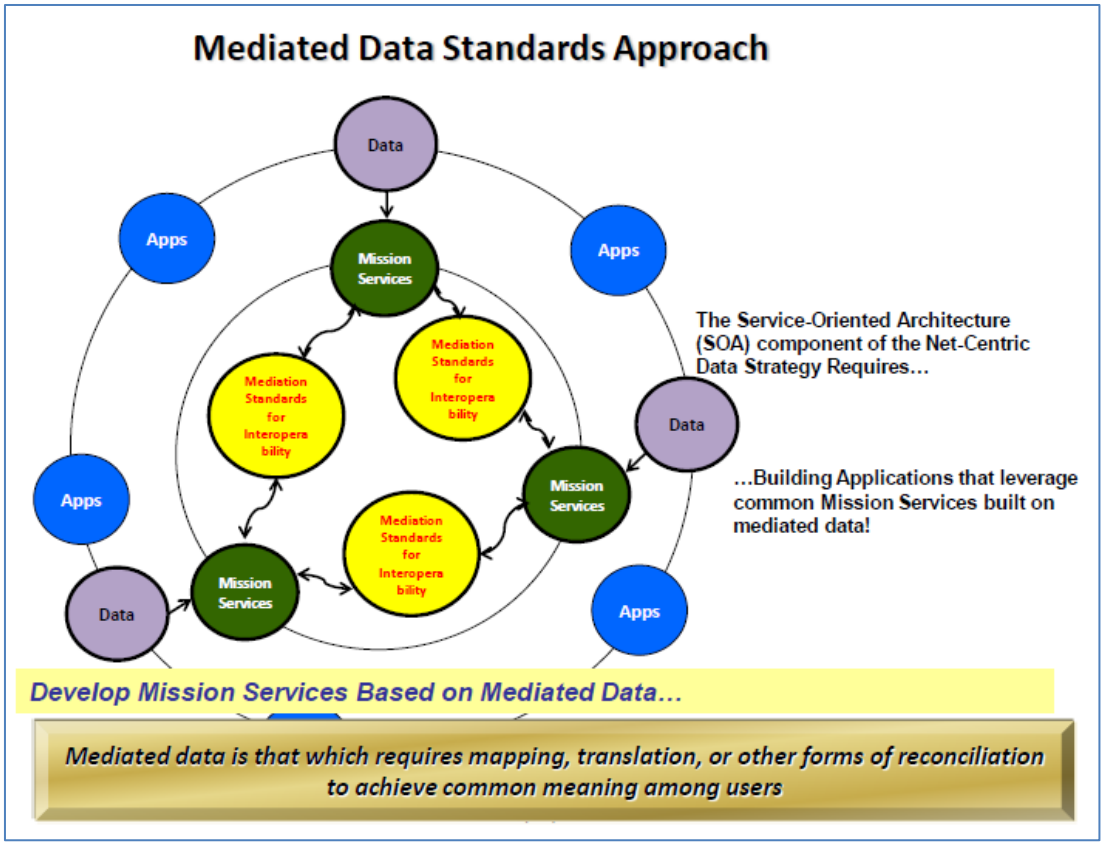

Figure 9 - Mediated Data Standards Approach

The mediated data approach is to accept vocabularies used in various IT systems and then do mappings, translations, and other forms of reconciliation that reflect agreement on the common meaning of terminology, thus enabling interoperability.

The process used by the Program Manager Mission Command (PM MC) is depicted in Figure 4. The process starts with existing vocabularies in individual IT systems. Then these IT systems connect to a server that provides a mediation capability such as the Publish and Subscribe Service (PASS) or the Data Dissemination Service (DDS) which are used to map terms. The result is an exchange of data and information based on agreed to semantic mappings.

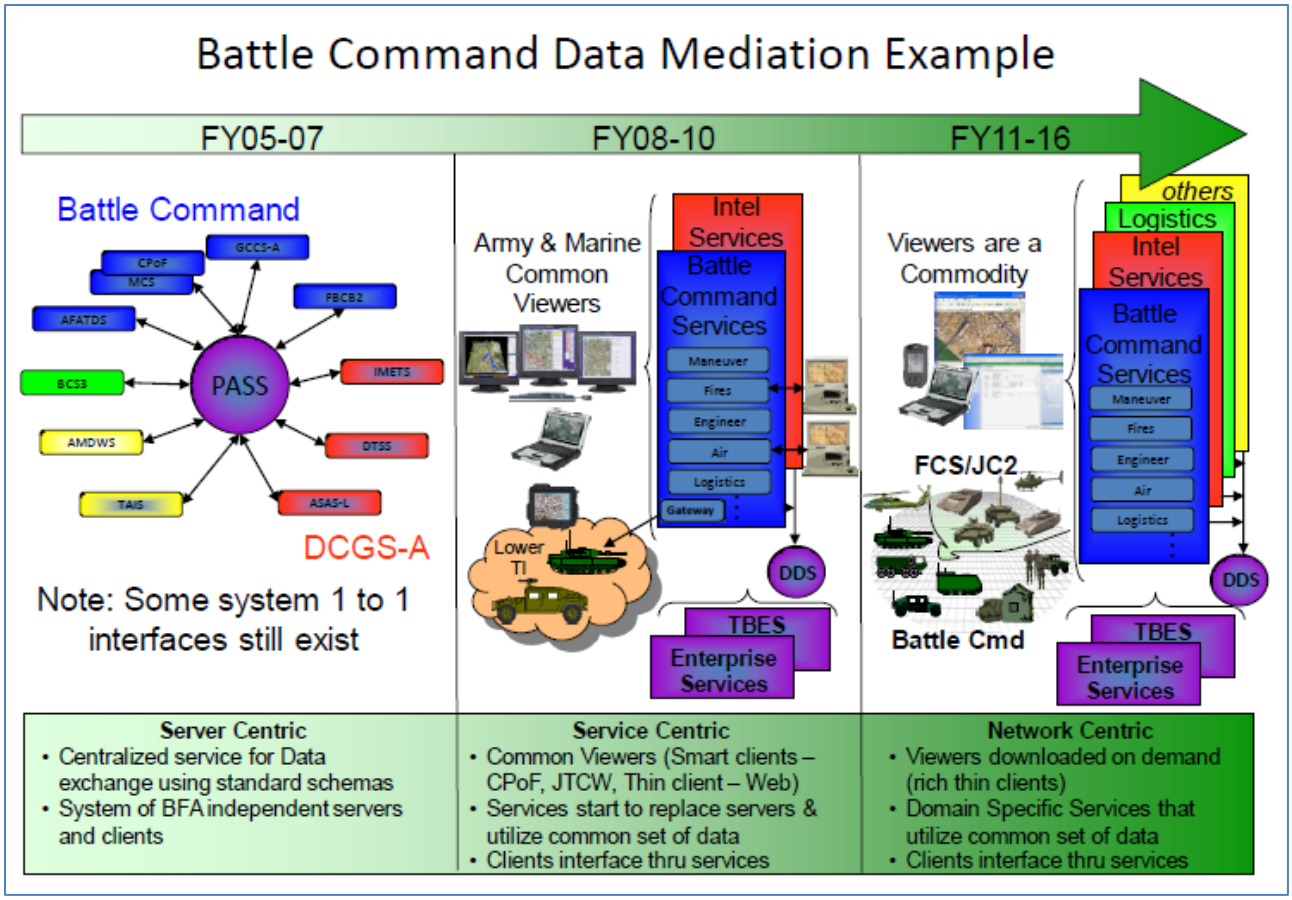

Figure 10 - Mission Command Data Mediation Process

4.3.2 Data Call Alternatives

A formal data call was issued to the COE CEs leadership. Questions were developed to address the study questions listed in Section 3.2. Data received were analyzed and the results are in a spreadsheet in Appendix D. The data call questions are:

1) What Automated Information Systems (AIS) focused Programs of Record (POR), Quick Response Capability (QRC) or non-POR activities are you responsible for developing or testing.

2) What missions or mission areas (e.g. Joint Capability Area (JCAs), Joint Mission Threads (JMTs, Functional Areas) does your Program support?

3) What data models (e.g. conceptual, logical or physical) have you used to help design, develop, and test your Program?

4) Have any of the data models used to answer question 3 captured the meaning (semantics) of the vocabularies and terminology used by the Program?

a) If so;

i) What standards (e.g. JC3IEDM, UCore, and NIEM) were used to develop the data dictionaries, metadata repositories or lexicons that support the data models?

ii) What high-level document (e.g., organizational doctrine; concepts of operation; tactics, techniques and procedures (TTPs)) do the data models represent?

iii) What forums (e.g. Working Groups, COIs) did you use or establish to develop the agreed upon vocabularies?

iv) Is there a configuration management process document for your program's data models?

v) Are there procedures and certification tools that test for system compliance with your data models?

vi) Were the data models used in the testing phases of the program (e.g. DOT&E and OT&E) to verify and certify semantic interoperability with other systems?

vii) What was the process you used to validate and certify semantic interoperability with other systems?

viii) Approximately, how much time and effort (e.g. man years) did it take to create the initial data models and test for semantic interoperability?

ix) Are the data models documented and available for review?

x) What improvements to policies, processes, and standards do you think would have made it easier (more efficient in terms of cost and schedule) to validate and certify semantic interoperability for you program?

b) If not;

i) How did you identify terminology used internally within your Program's software applications/application services? Were you able to exchange data (e.g. messages) between systems?

ii) What process did you used to validate and certify semantic interoperability between your program and other systems?

Data Call Findings

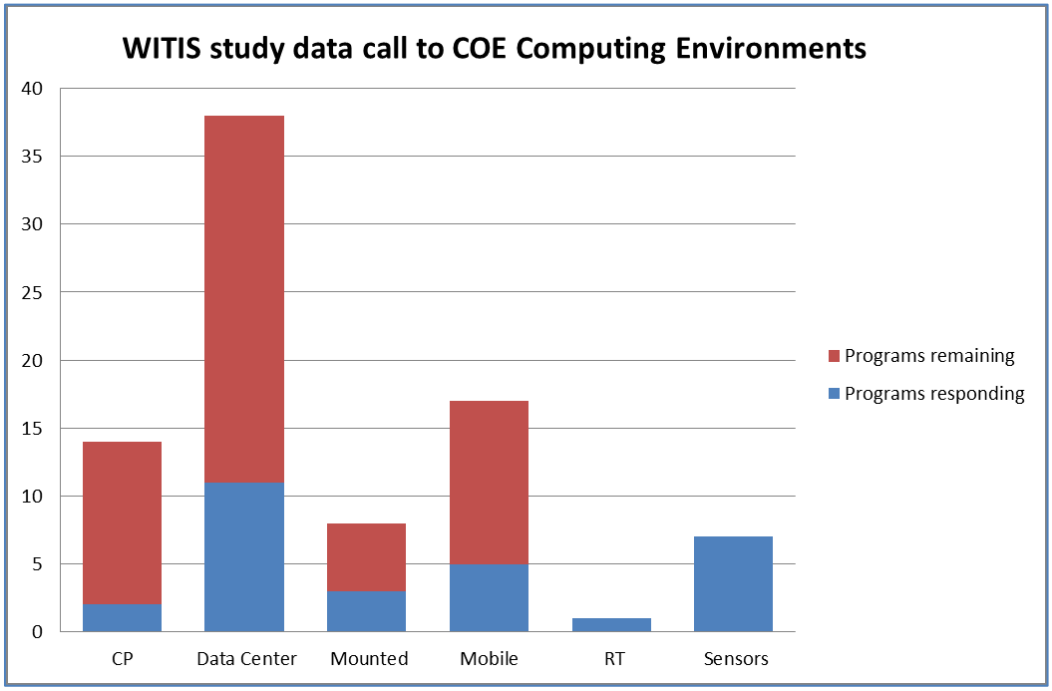

Figure 11 - Data Call Responses

Figure 11 shows that responses were receive from about 40 percent of the 80 Warfighting and supporting IT systems listed in the COE computing environment execution plans as shown in figure 11. The Sensor computing environment contains only IT systems that are part of other computing environments, so the response was counted as 100 percent.

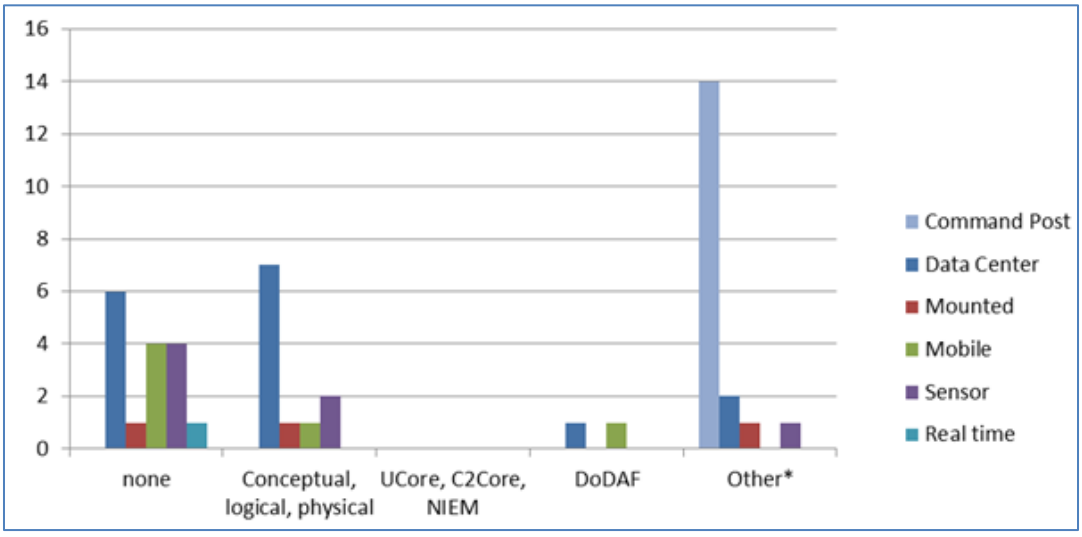

Figure 12 - Types of Data Models Used by COE Computing Environment Programs

Figure 12 shows five categories of data models used by the COE computing environments and the number of responses received in each category. The categories "none" and "other" were based on the responses to question 3 above; "What data models (e.g. conceptual, logical or physical) have you used to help design, develop, and test your program?" The DoDAF category was listed separately from the conceptual, logical, and physical category because two IT programs identified DoDAF explicitly in their responses.

This sample of responses is large enough to verify that the full population of IT programs is using a variety of standard data models to help with either mediation or development of common vocabularies to achieve semantic interoperability. Based on a normal distribution, at a 95 percent confidence level, the sample shows that about 30 percent of the programs use conceptual, logical, and/or physical data models to help achieve semantic interoperability. The margin of error (confidence interval) is about plus or minus 11 percent.

4.3.2.1 Analysis of Alternative Standards Pros and Cons

The analysis of pros and cons of standards was done based on the functional categories of standards described in Section 4.2.3 of the report. Pros and cons are described in Appendix C of this report. Results of the analysis are:

Vocabularies and Terminology

1) Warfighting doctrine which includes the *DoD Dictionary of Military and Associated Terms* enables common understanding across military forces because Warfighters are educated and trained based on doctrine.

2) Obtaining agreement through use of a COI or other authoritative body on a set of common data in the form of a standard dictionary or lexicon creates efficiency and effectiveness because there is a single starting point for achieving IT interoperability.

Data Models and Ontologies

1) Standards and standard tools for creating data models such as conceptual and logical models help to ensure accuracy and traceability to the semantic meaning of data as well as reusability when a community needs to expand its vocabulary.

2) Standards and standard tools for creating ontologies that show relationships among data can increase semantic understanding and repeatability across domains.

Architectures

DoD information architectures (e.g. Information Enterprise Architecture (IEA)) contain mostly principles and rules for data mediation and exchange of data, not standards for creating common data.

Repeatable Processes

Standards for repeatable end-to-end processes work more effectively and efficiently when user and developer collaboration begins early on in a process.

Authoritative Data Sources Including Repositories

1) Standards for authoritative data sources (ADSs) are particularly important during the first steps in the processes that lead to semantic IT interoperability.

2) Repositories are most useful when they allow the user to access and discover in a few minutes something of value.

4.3.2.2 Priorities of Alternative Standards

Priorities resulting from analysis of the pros and cons findings in the categories described in Section 4.2.3 are:

Vocabularies and Terminologies

Attention is required for standard criteria in order to establish common data dictionaries and lexicons.

Data Models and Ontologies

Use of logical data model and ontology standards appear to save time in creating unambiguous exchange schema.

Architectures

Additional semantic policy and front-end process standard criteria can facilitate improved IT interoperability.

Repeatable Processes

A standard for repeatable “semantics first” process is needed.

Authoritative Data Sources Including Repositories

Policy and process standards for authoritative bodies that address approval of authoritative data sources are needed to support IT interoperability within a COI or similar community.

4.4 Answers to Study Questions

1. What is the current status of data interoperability standards (e.g., data models)?

   Answer - Standards for two alternative approaches to achieving data commonality have been identified. The key standards associated with each approach described in Section 4.3.1 of this report are 1) policies and processes for establishing common data as an initial step before introducing the data into an IT system and 2) policies, processes, and technical standards for mediating the data exchanged among IT systems. Policy, process gaps, and issues associated with establishing data commonality standards have been identified from literature search, informal PM contacts, and Warfighter interviews. Use-case analysis and a formal data call (see appendices C and D) describe how IT programs are achieving data commonality.

2. How well do Army Warfighter systems comply with those standards?

   Answer – Use-case data collected and IT systems responses to a data call reported compliance with a variety of DoD and commercial standards for exchanging data and information. There are relatively few standards that are used to achieve semantic IT interoperability.

3. How well do the standards meet the interoperability needs of the warfighting area?

   Answer - According to Warfighter interviews and use-case and data-call analysis, additional data-commonality standards, in the form of policies, processes, and procedures, need to be developed and implemented if Warfighter needs are to be met.

4. What are the steps in the process of establishing a set of interoperability standards?

   Answer - DoD policy, architecture, and governance directives and instructions specify the steps to review, coordinate, and approve IT interoperability standards at the DoD level through the CIO Executive Council and its subgroups shown in Figure 13. Steps to locate, access, and choose appropriate existing and emerging standards are mostly left up to designated authoritative bodies to determine.

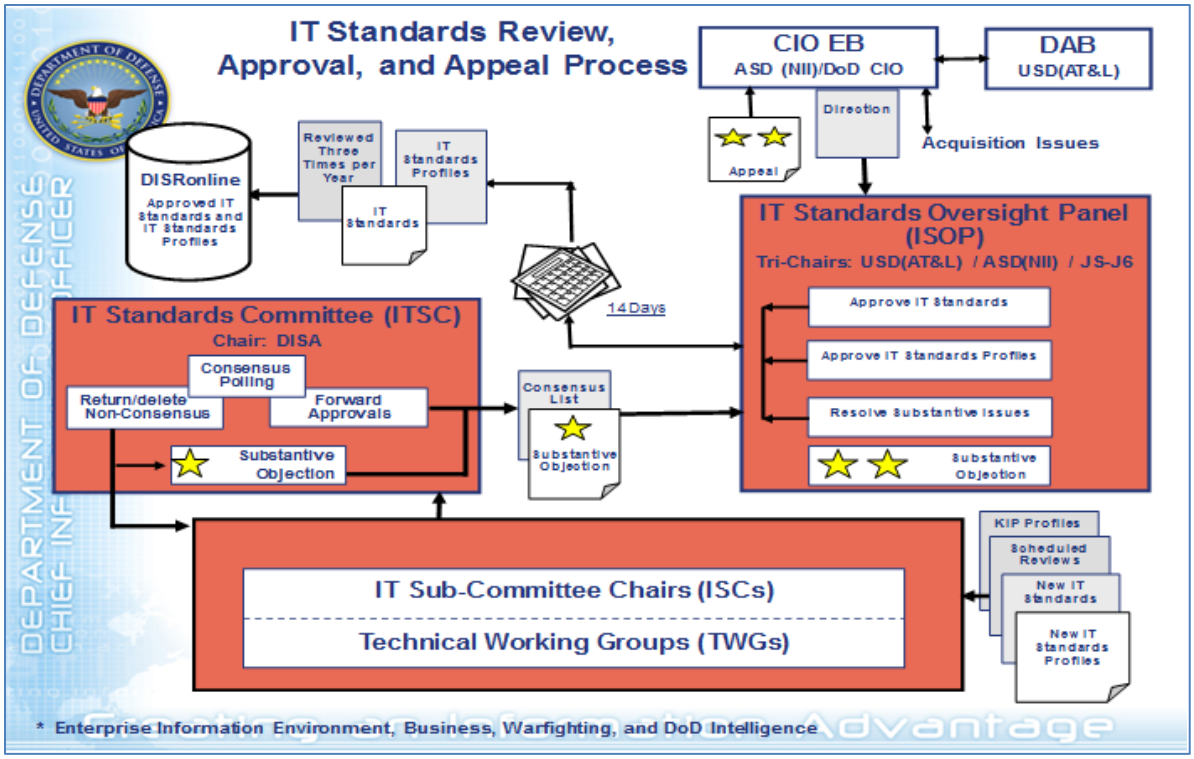

Figure 13 - DoD IT Standards Review, Approval, and Appeal Process

5. What organizations are responsible for executing each step?

Answer - At the DoD level, the CIO organization in OSD has overall responsibility for the steps in a process of reviewing and approving proposed DoD IT interoperability standards. In the Army, the CIO/G-6 has overall responsibility for approving IT interoperability standards. The policy for review and approval of IT interoperability standards is contained in Army Regulation 25-1. Other designated authoritative bodies such as the Army Data Board and communities of interest may select IT interoperability standards but there appears to be no overall process in the Army for doing so.

6. What information do they need to carry out each step, and where does that information come from?

Answer - Currently there are no official criteria in the Army for choosing IT interoperability standards. The Army Information Architecture contains sets of business rules and principles for exchange of data and information.

7. What alternatives to the recommended interoperability standards are already available?

Answer - The recommendations from this study offer alternatives to available standards in the form of identifying criteria that may be used to set standards for achieving both semantic and syntactic IT interoperability.

8. What is their level of maturity, and the cost and applicability?

Answer - The alternative policy and process standards have to be developed, coordinated, and approved. At this time, the JAMD use case has information that shows increases in efficiency is realized using their common data approach, but an analysis of this data was not done in this study. A business-case analysis needs be performed to verify and document how much time, effort and costs can be avoided.

Section 5 - Recommendations

5.1 Recommendations Introduction

Recommendations from this study are intended to address gaps and issues described in Section 4.1 of this report. The recommendations are based on findings from analysis of use cases, data call results, discussion with Warfighters, and best practices in IT programs found in a literature search. These recommendations are meant primarily to help the Army CIO/G-6 and ASA(ALT) organizations develop and implement policies and processes which can be used as standards to support IT interoperability. However, the authors believe that recommendations contained in this report also are applicable to the broader DoD enterprise since Army Warfighting and supporting IT systems have to function, in general, in a Joint, Interagency and coalition environment.

Overall, a recommendation is made to improve the way program executive offices, program managers, communities of interest, and other groups discover, locate, select, and access IT interoperability standards both for exchange as well as semantic purposes. We strongly encourage the development and approval of policies and processes that contain criteria which enable users to select and use appropriate IT interoperability standards and which specify metrics that can be used to evaluate how well those standards help achieve IT interoperability.

Questions that may be useful in developing policies and processes that specify criteria for choosing semantic IT interoperability standards are contained in the recommend-dations below.

Our specific recommendations are grouped into the five categories of standards identified in Section 4.2.3 of this study. They are:

5.2 Vocabularies and Terminology Recommendations

The development of vocabularies and terminology used for interoperability purposes should be based on the use of operational concepts and doctrine that apply to the mission that the IT system supports. This should be done as soon as the need for the IT system is identified in order 1) to better ensure a common understanding of the vocabularies and terminology is achieved and 2) for efficiency to occur in the development process. Gaining agreement on terminology is time consuming. So, only that portion of the vocabulary needed for interoperability should be given the time and effort to obtain agreement on the meaning of terminology, create vocabularies and terminology, and documenting vocabularies and terminology in, for example, dictionaries and lexicons.[21]

Standard processes for creating vocabularies and terminology are not identified in existing DoD policies. However, the following questions may be useful in developing criteria for creating and/or choosing standards for vocabularies and terminology that help achieve IT interoperability from a semantic perspective.

- Does the standard process allow the vocabulary to encompass enterprise terminology needed for interoperability across appropriate domains?

- Does the standard process require the terms in the vocabulary to be unambiguously defined?

- Does the standard process require the vocabulary to be based on authoritative information (e.g. doctrine)?

- Does the standard process promote commonality among vocabularies of systems that need to interoperate with one another?

- Can the standard process be used to help measure the level of interoperability?

Vocabularies, terminology, and associated standards should be *required* to be approved by authoritative bodies as noted in DoD and Army policies so that existing as well as future developers of vocabularies and terminology can leverage previous work where appropriate. See the section on authoritative data sources and repositories below for related recommendations on this topic.

5.3 Data Models and Ontologies Recommendations

Guidance should be provided to IT developers as to where the use of data models and ontologies are needed so as to help standardize the way IT interoperability, from a semantic perspective, is designed and tested.

In some instances, a logical data model may be sufficient to organize the taxonomies and relationships among information shared for use by Warfighters. In more complex situations a more structured ontology may be needed to describe relationships among data and information shared for interoperability purposes.

Standard data models that describe the semantics of shared information exist for DoD and the Federal government and should continue to be developed (i.e., matured) and used in accordance with Warfighter doctrine and training. Among these models are NIEM, UCORE. Top-level container models such as UCore should be complemented by more detailed models such as C2 Core. Governance of these models should follow in a federated approach. Data models such as JC3IEDM, which was created specifically for sharing C2 information by Joint and coalition Warfighters, should be leveraged to reduce implementation times.

As in the case of vocabularies and terminology, data models and ontologies should be required to be approved by authoritative bodies as noted in DoD and Army policies so that users of existing and future data models and ontologies can leverage previous work where appropriate.

The following questions may be useful criteria when creating and/or choosing standard processes for creating data models and ontologies that support IT semantic interoperability.

- Does the standard allow the model to contain an acceptable (to an appropriate authoritative body) set of data and relationships in the domain?

- Does the standard require the model to be extensible and accommodate relationships among domains?

- Does the standard allow the model to leverage other open, commercial, and government standards?

- Does the standard require the model to be maintained, documented, and used for interoperability certification and validation?

- Does the standard allow the model to be used as part of an overarching container model such as UCORE and/or NIEM?

- Can the standard be used to help measure the level of interoperability?

5.4 Architecture Recommendations

Army policies, principles, and standards that apply to the creation and use of common data and information (as defined in this report) in IT systems that support Warfighter interoperability should be augmented by architectural guidance on establishing data and information commonality.

Specifically, the Army authoritative sources such as AR 25-1 and DAPAM 25-1-1 should contain processes and criteria that can help authoritative bodies such as COIs choose standards for achieving data commonality from a common data and/or a mediation approach described in Section 4.3.1 of this document.

The following questions are provided for helping to develop criteria for creating and/or choosing standards for Army architectures that support IT interoperability.

- Does the standard require the architecture to capture both the semantic and syntactic elements of IT interoperability?

- Does the standard allow the architecture be used to design, test, and evaluate activities that measure the degree of interoperability between IT systems?

- Does the standard require that the architecture be documented and considered to be (by an appropriate COI) extensible for future changes?

- Does the standard allow the architecture be used to help measure the degree of IT interoperability (as defined in CJCSI 6212.01F, “Net Ready Key Performance Parameter”) among IT systems?

5.5 Repeatable Process Recommendations

Army policy in the AIA, AR 25-1, and DAPAM 25-1-1 should describe a repeatable process that describes the end-to-end lifecycle for identifying solutions to achieve needed IT interoperability. The process should include design, development and testing of the data and information contained in IT systems that support Warfighter interoperability. Policy that can be derived from results of prototype efforts such as the Army C2 Core Data Sharing Pilot and the Tactical Edge Data Solutions (TEDS) pilots should be leveraged. Metrics should be developed to assess how well the repeatable process works in improving the effectiveness and efficiency of IT interoperability.

The following questions are provided for use in developing criteria for creating and/or choosing standards for repeatable processes to support IT interoperability from a semantic perspective.

- Does the standard require the process to encompass all the activities from data creation through data exchange and archiving (i.e., is it an end-to-end process)?

- Does the standard require the process to be repeatable in a way that it can be measured?

- Does the standard require the process to save time and effort compared to existing ways of accomplishing IT interoperability?

5.6 Authoritative Data Sources and Repositories Recommendations

Army authoritative bodies (ABs), such as the Army Data Board, that approve authoritative data sources should be used for functional areas such as the Army COE. The ABs should require authoritative data sources they approve to be included in DoD registries such as the EADS Registry. Registries should be required to provide linkages to the authoritative data that can be accessed on a need-to-know basis. Policies that identify where to find authoritative data sources and repositories that contain standards for vocabularies and terminology, data models and ontologies, architectures, and repeatable processes should be contained in Army architecture policy and other appropriate Army documents.

The following questions are provided for use in developing criteria for creating and/or choosing standards for authoritative data sources and repositories that support IT interoperability from a semantic perspective.

- Does the standard process require that an authoritative body has certified the ADS as the official source for a particular kind of information?
- Does the standard require that the ADS is a single source for that type of data?

- Does the standard require that the ADS reliable and trustworthy?

- Does the standard require that the data are being maintained in accordance with policies and procedures that govern authoritative data sources (ADSs)?

- Does the standard require that the repository be accessible in near real time?

- Does the standard require that data in a repository be found within an acceptable amount of time to most users?

- Can the standard be used to help measure the level of interoperability?

This page intentionally left blank.

Section 6 - Conclusions

The authors believe that the results and recommendations of this study can lead to opportunities to create efficiencies in IT development and operation by Warfighters and supporting organizations. The evidence presented in this study indicates that simpler and less costly IT systems probably can be implemented to support interoperability if standard policies, processes, and procedures that include semantic IT interoperability guidance are developed and approved as part of an alternative to existing policies and processes. Furthermore, we believe that criteria for choosing standards can make it easier to modify IT systems for interoperability purposes in the future.

All of these recommended changes to policies, processes, and procedures will take time to implement because of the socialization needed to achieve buy in. But, given this era of dwindling defense budgets, alternatives to the current approaches to achieve IT interoperability should be investigated for their effectiveness and efficiency. We believe that the results of this study can be used to assist DoD officials participating in development of the new DoD data framework requested in the 29 June memorandum.[4]

This page intentionally left blank.

Endnotes

[1] US and Coalition Forces Data(Semantic) Interoperability Study, Institute for Defense Analyses document D-4018, Jan. 2010
[2] A prototype to Deliver IT Interoperability Study, Institute for Defense Analyses document D-4198, Oct. 2010
[3] Information Technology Management Reforms memorandum, Sec. Army, Sep. 8, 2011
[4] DoD Data Framework, Deputy Assistant Secretary of Defense (C3 & Cyber) memorandum entitled, June 29, 2012
[5] Unmanned Aircraft Systems Interoperability Initiative, Capabilities Based Assessment, Final Report, Director, Unmanned Warfare, OSD (AT&L) May 14, 2012
[6] DoD Net-Centric data strategy memorandum, DoD CIO, May 9, 2003
[7] Sharing Data, Information, and Information Technology (IT) Services in the DoD Directive 8320.02, June 1, 2011
[8] DoD Information Enterprise Architecture, version 1.2, May 7, 2010
[9] LTG Susan Lawrence, Town hall meeting presentation Nov. 9, 2011, the Pentagon
[10] Army CIO/G-6, LandWarNet Powering America's Army, October 2011
[11] Weapons Technical Intelligence Improvised Explosive Devices Lexicon, DIA and JIEDDO, version 2.0, December 2008
[12] UCORE and NIEM; Creating Potent New Cross-Boundary Networks, Office of Program Manager ISE, www.ise.gov
[13] Command and Control (C2) Core Maturation and Implementation Guidance, OSD NII memorandum, March 12, 2010
[14] UCORE Way Ahead Hybrid Option briefing, Defense Information Services Agency, Oct. 19, 2011
[15] DoD Architecture Framework Version 2.02, DoD Deputy Chief Information Officer, May 2012
[16] DoD Business Operations draft Technical Transition Plan, version .992,Deputy Chief Management Office, Sept. 2011
[17] Army Field Manual 5-0, Army Planning and Orders Production, Sec. 4-1, Jan. 2005
[18] LTC William Mandrick, Guide to a Repeatable Process for Ontology Creation, William.Mandrick@us.army.mil
[19] Semantics First for C2 Core Repeatable Process, Army CIO/G-6, AONS, Apr. 7, 2011
[20] Chairman, Joint Chiefs of Staff Instruction 6112.01F, Net Ready Key Performance Parameter, Mar. 21, 2012
[21] This recommendation is based on discussions of lessons learned with the Joint Air and Missile Defense COI POC David Skidmore and with the DoD ICODES developer, Jens Pohl

This page intentionally left blank.

Appendix A – References

DoD Issuances

Department of Defense Directive (DoDD) 4630.05, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”

DoDD 5015.2, “DoD Records Management Program”

DoDD 8000.01, “Management of the Department of Defense Information Enterprise”

DoDD 8115.01, “Information Technology Portfolio Management”

DoDD 8320.02, “Sharing Data, Information, and Information Technology Services in the DoD”

DoDD 8320.03, “Unique Identification (UID) Standards for a Net-Centric Department of Defense”

Department of Defense Instruction (DoDI) 4630.8, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)”

DoDI 5025.12, “Standardization of Military and Associated Terminology”

DoD Net-Centric Data Strategy memorandum, DoD CIO, May 9, 2003

“DoD Information Enterprise Architecture”, version 1.2, May 7, 2010

DoD Architecture Framework (DoDAF) Version 2.02, DoD Deputy Chief Information Officer, May 2012

“DoD CIO Executive Board Charter” memorandum signed February 12, 2012 (http://dodcio.defense.gov/Portals/0/Documents/Announcement/001_Signed%20DoD%20CIO%20ExBd%20Charter%2002-12-2012%20.pdf”)

DoD Business Operations draft Technical Transition Plan, version .992, Deputy Chief Management Office, Sept. 2011

“Command and Control (C2) Core Maturation and Implementation Guidance”, OSD NII memorandum, March 12, 2010

Chairman of the Joint Chiefs of Staff Issuances

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5120.02C, “Joint Doctrine Development System”

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 5120.01, “Joint Doctrine Development System”

CJCSI 5705.01D, “Standardization of Military and Associated Terminology”

CJCSI 6112.01F, “Net Ready Key Performance Parameter”, Mar. 21, 2012

CJCSI 8410.01A, “Warfighting Mission Area Information Technology Portfolio Management and Net-centric Data Sharing”

Joint Publication (JP) 1, “Doctrine for the Armed Forces of the United States”

JP 1-02, “DoD Dictionary of Military and Associated Terms”

JP 3-01, “Countering Air and Missile Threats”

US Army Documents

Army Regulation (AR) 25-1, “Army Knowledge Management and Information Technology”

Department of the Army Pamphlet, 25-1-1, “Information Technology Support and Services”

“Information Technology Management Reforms” memorandum, Secretary of the Army, Sep. 8, 2011

Army CIO/G6 ASA(ALT) “Common Operating Environment Architecture Guidance” memorandum, Oct. 20, 2010

“Common Operating Environment Implementation Plan”

“LandWarNet: Powering America’s Army” (http://ciog6.army.mil/LinkClick.aspx?fileticket=ONAWePgetXo%3d&tabid=36)

“Army Information Architecture”

Army Field Manual (FM) 5-0, “Army Planning and Orders Production”, Sec. 4-1, Jan. 2005

Defense Information Systems Agency Document

“UCORE Way Ahead Hybrid Option” briefing, Defense Information Services Agency, October 19, 2011

Institute for Defense Analyses Documents

US and Coalition Forces Data (Semantic) Interoperability Study, Institute for Defense Analyses document D-4018, Jan. 2010

A Prototype to Deliver IT Interoperability Study, Institute for Defense Analyses document D-4198, Oct. 2010

Defense Intelligence Agency Document

“Weapons Technical Intelligence Improvised Explosive Device Lexicon”, DIA and JIEDDO, version 2.0, Dec. 2008

Information Sharing Environment Document

“UCORE and NIEM; Creating Potent New Cross-Boundary Networks”, Office of Program Manager ISE, www.ise.gov

This page intentionally left blank.

Appendix B – Glossary

Part 1 - Abbreviations and Acronyms

Acronym	Full Name
A	
AALPS	Automated Air Load Planning System
ABCS	Army Battle Command System
ACQBIZ	Acquisition Business
ADS	Authoritative data source
AESIP	Army Enterprise Systems Integration Program
AFATDS	Advanced Field Artillery Tactical Data System
AHLTA	Armed Forces Health Longitudinal Technology Application
AHRS	Army Human Resource System
AIA	Army Information Architecture
AIS	Automated Information Systems
AKO	Army Knowledge Online
ALMS	Army Learning Management System
ALTESS	Acquisition, Logistics and Technology Enterprise Systems and Services
AMDWS	Air and Missile Defense Work Station
AMFT-ITV	Automated Movement Flow Tracking In-Transit Visibility
AMPS	Aviation Mission Planning System
AMR	Air Movement Request
ANSI	American National Standards Institute
API	Application Programming Interface
AR	Army Regulation
ASA(ALT)	Assistant Secretary of the Army, Acquisition. Logistics and Technology
ASCOPE	Area, Structures, Capabilities, Organizations, People, and Events
ASD(NII)	Assistant Secretary of Defense (Networks and Information Integration)
ATO	Authority to Operate
B	
BAT-A	Biometric Automated Toolset - Army
BCCS	Battlefield Command and Control System
BCS3	Battle Command Sustainment and Support System
BCT	Brigade Combat Team
BEC	Biometrics Enabling Capability
BFO	Basic Formal Ontology

C

C2	Command and Control
C2Core	Command and Control Core
C3T	Command, Control and Communications
CADIE	Capability Architecture Development and Integration Environment
CDD	Capability Development Document
CE	Computing Environment (of the Common Operating Environment)
CHARCS	Counterintelligence Human Intelligence Automated Reporting and Collection System
CIDNE	Combined Information, Data, Network, Exchange
CHESS	Computer Hardware, Enterprise Software and Solutions
CMD-P	Computer Meteorological Data Profiler
COE	Common Operating Environment
COI	Community of Interest
CIDS	Common International Air and Missile Defense Data Set
CIO	Chief Information Officer (CIO)
CIO EB	DoD CIO Executive Board
CIO/G-6	Army Chief Information Officer/G-6
CIXS	Common International Air and Missile Defense XML Schema
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CMP	Configuration Management Plan
COE	Common Operating Environment
COI	Community of Interest
CP	Command Post
CPD	Capability Production Document
CPOF	Command Post of the Future
CUO	Common upper ontology

D

DAB	Defense Acquisition Board
DAPAM	Department of the Army Pamphlet
DARS	DoD Architecture Registry System
DCAT	Dynamic Collaborative Action Team
DCGS-A	Distributed Common Ground System – Army
DCMO	DoD Deputy Chief Management Office
DDS	Data Distribution Service
DDMS	DoD Discovery Metadata Specification
DHIMS	Defense Health Information Management System
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	DCGS Integration Backbone
DISR	DoD Information Technology Standards and Profile Registry
DITPR	DoD Information Technology Portfolio Repository
DISA	Defense Information Systems Agency
DoD	Department of Defense

DoD CIO	DoD Chief Information Officer
DoDI	Department of Defense Instruction
DOJ	Department of Justice
DLS	Distributed Learning System
DMS-A	Defense Messaging System - Army
DoDAF	Department of Defense Architecture Framework
DOT&E	Development and Operation Test & Evaluation
DOT&E	Director, Operational Test & Evaluation
DT&E	Developmental Test and Evaluation
DOTMLPF	Doctrine, Organization, Training, Material, Leadership and Education, Personnel and Facilities
DPP	Data performance plan
DPPS	Data performance plan system

E

EADS	Enterprise Authoritative Data Sources (Registry)
EDS-LITE	Enterprise Directory Service - Lite
EHR	Electronic Health Record
EID	Enterprise Identifier
EIS	Enterprise Information Services
EMT	Effects Management Tool
ENFIRE	Engineering Field Planning, Reconnaissance, Surveying, and Sketching Set
ES	Enterprise Services

F

FACE(TM)	Future Airborne Capability Environment
FBCB2	Force XXI Battle Command, Brigade-and-Below
FCS	Future Combat System
FEA	Federal Enterprise Architecture
FGDC	Federal Geographic Data Committee
FMS	Force Management System
FOS	Forward Observer System
FP	Force Protection
FSC2	Fire Support Command and Control

G

GCCS-A	Global Command and Control System – Army
GFEBS	General Fund Enterprise Business System
GNEC	Global Network Enterprise Construct

H

HR	Human Resource

I

IEA	DoD Information Enterprise Architecture
IEEE	Institute of Electrical and Electronics Engineers
IESS	Information exchange standard specifications
IEW&S	Intelligence, Electronic Warfare & Sensors
IMS-A	Installation Management Systems – Army
IPPS-A	Integrated Personnel and Pay System - Army
IPT	Integrated Product Teams
ISC	IT Sub-Committee Chair
ISO	International Organization for Standardization
ISOP	IT Standards Oversight Panel
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
ITSC	IT Standards Committee

J

J-AIT	Joint – Automatic Identification Technology
JADOCS	Joint Automated Deep Operations Coordination System
JAMD	Joint Air and Missile Defense
JBC-P	Joint Battle Command – Platform
JC2	Joint Command and Control
JC3IEDM	Joint Consultation, Command and Control Information Exchange Data Model
JCA	Joint Capability Area
JCB	Joint Capabilities Board
JCPAT-E	Joint C4I Program Assessment Tool-Empowered
JCR	Joint Capabilities Release
JDEIS	Joint Doctrine, Education, and Training Electronic Information System
JDES	Joint Data Engineering and Standardization
JEM	Joint Effects Mode
JIAMD	Joint Integrated Air and Missile Defense
JIEDDO	Joint Improvised Explosive Devices Defeat Organization
JIM	Joint, Interagency, Multinational
JITC	Joint Interoperability Test Command
JMIS	Joint Medical Information Systems Office
JMT	Joint Mission Threads
JPD	Joint Planning Document
JPI	Joint Personnel Identification System
JROC	Joint Requirements Oversight Council
JWARN	Joint Warning and Reporting Network

K

KLE	Key leader engagement
KM/DS	Knowledge Management and Decision Support

L

LHMBC	M32 Lightweight Handheld Mortar Ballistic Computer
LMP	Logistics Modernization Program

M

MBCOTM	Mounted Battle Command on the Move
MC DDS	Message Context Data Distribution Service
MC4	Medical Communications for Combat Casualty Care
MCS	Maneuver Control System
MCWS	Mission Command Workstation
MDI	Model, data, implement
MDMP	Military Decision Making Process
MDR	DoD Metadata Registry
MFLTS	Machine Foreign Language Translation System
MTS	Movement Tracking System
MIEM	Maritime Information Exchange Model
MIP	Multilateral Interoperability Programme
MOA	Memorandum of Agreement
MOS	Military Occupational Specialty

N

NETOPS	Network Operations
NIEM	National Information Exchange Model
NGS	NIPRNet Globe Services
NR KPP	Net ready key performance parameter
NSA	National Security Agency
NSS	National security system

O

ODNI	Office of the Director of National Intelligence
OSD (DCAPE)	Office of the Secretary of Defense (Director, Cost Assessment and Program Evaluation)
OGE	Operation Guardian Enable
OGE	Global Mission Network (part of GNEC)
ONS	Operational Needs Statement
ORD	Operational Requirements Document
OT&E	Operational Test and Evaluation
OWL	Web Ontology Language

P

PASS	Publish and Subscribe Service
PEO	Program Executive Office
PEO IEW&S	PEO Intelligence Electronic Warfare and Sensors
POR	Programs of Record
PPBE	Planning, Programming, Budgeting, and Execution

PTDS	Persistent Threat Detection System

Q

QRC	Quick Response Capability

R

RCAS	Reserve Component Automation Systems
RDF	Resource Description Framework
RFMSS	Range Facility Management Support System
RPIM	Real Property Information Model
RT	Real-Time
RTM	Requirements Traceability Matrix

S

SEC	Software Engineering Center
SED	Software Engineering Directorate
SEP	System Engineering Plan
SFIS	Standard Financial Information Structure
SIPRNET	Secret Internet Protocol Router Network
SLC	Service Life Cycle
SNaP-IT	Select and Native Programming Data Input System – Information Technology
STAMIS	Standard Army Management Information Systems
STP	System Tracking Program
STRATCOM	US Strategic Command

T

TAIS	Tactical Airspace Integration System
TC-AIMS	Transportation Coordinator's Automated Information for Movements System
TCM	TRADOC Capabilities Manager
TEDS	Tactical Edge Data Solutions
TIGR	Tactical Ground Reporting System
TIS	Transportation Information Systems
TMC	Tactical Mission Command
TMS	Tactical Messaging System
TTPs	Techniques, Tactics and Procedures
TWG	Technical Working Group

U

UCore	Universal Core
UK MOD	United Kingdom Ministry of Defense
USD(AT&L)	Under Secretary of Defense (Acquisition, Logistics, and Technology)
USMTF	US Message Text Format

V

VMF	Variable Message Format

W

W3C	World Wide Web Consortium
WG	Working Group
WIN-T	Warfighter Information Network – Tactical
WMA	Warfare Mission Area

X

XML	eXtensible markup language

This page intentionally left blank.

Part 2 – Terms and Definitions

Introduction

As this study was conducted, we found a need to improve the policy and process bearing on implementing interoperability among the IT systems used by warfighters (and others). Policy and process documents are particularly weak on guidance on terminology standardization among IT systems.

Because current policy and process documents bearing on semantic interoperability in IT systems use inconsistent terminology, the definitions listed below were often selected from several available in the various authoritative sources (e.g., DoD and Joint Staff issuances). When there were several definitions that could be included in this glossary, the criteria to select one was which definition contributed most to creating a framework that facilitates understanding how to create the semantic interoperability needed to realize the vision explained in Joint Requirements Oversight Council Memorandum (JROCM) 134-01, "Capstone Requirements Document: Global Information Grid," and in the "DoD Net-Centric Data Strategy."

To facilitate readers' understanding the policy and process problem, the first four definitions below are for the term, *interoperability*. A member of the senior executive service observed about the multiple definitions of interoperability: "We haven't even got interoperability on the definition of interoperability."

Interoperability
1. The ability to operate in synergy in the execution of assigned tasks. (Joint Publication [JP] 3-0, *Joint Operations*)
2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases. (JP 6-0, *Joint Communications System*) (both definitions are included in JP 1-02, *DoD Dictionary of Military and Associated Terms*)

Interoperability
The ability to operate in synergy in the execution of assigned tasks. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/ or their users. The degree of interoperability should be defined when referring to specific. (JP 1-02) For IT (and NSS), interoperability is the ability of systems, units or forces to provide data, information, materiel and services to and accept the same from other systems, units or forces and to use the data, information, materiel and services so exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the operational effectiveness of that exchanged information as required for mission

accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the lifecycle and must be balanced with IA. (CJCSI 6212.01F, “Net Ready Key Performance Parameter (NR KPP)”)

Interoperability
Ability of elements within an information system to communicate with each other and exchange information. Interoperability non-exclusively references data formats, signal levels, physical interface characteristics, logical or relational alignments, and transmission methods or media types. *(DoD Information Enterprise Architecture*)

Interoperability
The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations and missions over the life cycle and must be balanced with information assurance. (DoDD 4630.05)

Architectures
The structure of components, their relationships, and the principles and guidelines governing their design and evolution over time. (DoDD 4630.05)

Authoritative Data Source
A recognized or official data production source with a designated mission statement or source/product to publish reliable and accurate data for subsequent use by customers. An authoritative data source may be the functional combination of multiple, separate data sources. (DoDD 8320.03)

Capability
The ability to execute a specified course of action. It is defined by an operational user and expressed in broad operational terms. A capability includes the doctrine, organization, training, materiel, leadership and education, personnel, and facilities required to achieve a specified course of action. (DoDD 4630.05)

Capability Gaps
Those synergistic resources (DOTMLPF) unavailable, but potentially attainable to the operational user for effective task execution. (DoDI 4630.8)

Capability-Focused, Effects-Based Interoperability

Interoperability process that:

- Includes experts from the operational community to identify, consolidate and prioritize interoperability needs; and synchronize non-materiel solutions with materiel solutions for both new and fielded capabilities.
- Characterizes IT and NSS interoperability needs in a capability-focused, effects-based context using integrated architectures derived from Joint Operating Concepts (JOCs) and Joint Functional Concepts (JFCs).
- Assesses net-readiness; information assurance requirements; and both the technical exchange of information and the end-to-end operational effectiveness of that exchange using the NR-KPP.
- Incorporates both materiel (acquisition or procurement) and non-materiel (doctrine, organization, training, leadership and education, personnel, or facilities) solutions.
- Verifies interoperability solutions in formal tests or operational exercises.
- Continuously verifies the NR-KPP and evaluates overall IT and NSS interoperability, within a given capability, throughout a system's life. (DoDD 4630.05 and DoDI 4630.8)

Common Operating Environment

An approved set of computing technologies and standards that will enable secure and interoperable applications to be developed rapidly and executed across a variety of computing environments: server, client, mobile devices, sensors and platforms. It is an Army effort consisting of an Army's plan to modernize equipment and weapons systems around a common set of IT standards and architecture as it develops a truly networked force. (Deputy Chief of staff, G-3/5/7, execution Order: Army Enterprise Common Operating Environment (COE) Convergence Plan (24 May 2010)

Department of Defense Information Enterprise

The DoD information resources, assets, and processes required to achieve an information advantage and share information across the Department of Defense and with mission partners. It includes: (a) the information itself and the Department's management over the information life cycle; (b) the processes, including risk management, associated with managing information to accomplish the DoD mission and functions; (c) activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and (d) related information resources such as personnel, funds, equipment, and IT, including national security systems. (DoDD 8000.01)

DoD Enterprise-Level

Relating to policy, guidance, or other overarching leadership provided by OSD Officials and the Chairman of the Joint Chiefs of Staff in exercising authority, direction, and control of their respective elements of the Department of Defense on behalf of the Secretary of Defense. (DoDD 8000.01)

DoD Enterprise Architecture
A federation of descriptions that provide context and rules for accomplishing the mission of the Department. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define the people, processes, and technology required in the “current” and “target” environments; and the roadmap for transition to the target environment. (DoDD 8000.01)

DoD Information Technology Standards Registry (DISR)
The DISR provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements. It defines the service areas, interfaces, standards (DISR elements), and standards profiles applicable to all DoD systems. Use of the DISR is mandated for the development and acquisition of new or modified fielded IT and NSS systems throughout the Department of Defense. The DISR replaced the Joint Technical Architecture. (DoDD 4630.05 and DoDI 4630.8)

Enterprise Solution
The action of solving a problem or satisfying a requirement that affects the entire organization (e.g., Department of Defense). (DoDD 8000.01)

Entity
An independent unit or distinguishable person, place, thing, event, or concept about which information is kept that has distinct features, objects, or attributes associated with it. (DoDD 8320.03)

Evaluation (Evaluate)
Measuring or quantifying the value, characteristics, or capabilities of something against established standards, (as in "Test and Evaluation"). The determination of, or act of determining the relative degree to which IT and NSS interoperability is achieved. (DoDI 4630.8)

GIG
The Global Information Grid globally interconnected end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems. Non-GIG IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network. (DoDD 8000.01) (Note that this definition includes data within the GIG)

Global Information Grid (GIG) Key Interface Profiles (KIPs)
GIG KIPs provide a net-centric oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces. The KIP is the set of documentation produced as a result of interface analysis which designates an interface as key; analyzes it to understand its architectural, interoperability, test and CM

characteristics; and documents those characteristics in conjunction with solution sets for issues identified during the analysis. GIG KIPs provide a description of required operational functionality, systems functionality and technical specifications for the interface. The profile consists of refined operational and systems view products, Interface Control Document/Specifications, Engineering Management Plan, CM Plan, TV-1 with SV-TV Bridge, and procedures for standards conformance and interoperability testing. An interface is designated as a key interface when one or more the following criteria are met:
The interface spans organizational boundaries.

- The interface is mission critical.
- The interface is difficult or complex to manage.
- There are capability, interoperability, or efficiency issues associated with the interface.
- The interface impacts multiple acquisition programs.
- The interface is vulnerable or important from a security perspective.

Information
Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. (DoDD 8000.01) (Note that this definition includes data within information. That is, the definition does not make a distinction between data and information.)

Information Assurance (IA)
Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DoDD 4630.05)

Information Needs
A condition or situation requiring knowledge or intelligence derived from received, stored, or processed facts and data. (DoDD 4630.05 and DoDI 4630.8)

Information Support Plan (ISP)
The identification and documentation of information needs, infrastructure support, IT and NSS interface requirements and dependencies focusing on net-centric, interoperability, supportability and sufficiency concerns. (DoDI 4630.8)

Information Technology (IT)
Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the Executive Agency. This includes equipment used by a DoD Component directly, or used by a contractor under a contract with the DoD Component, which requires the use of such equipment, or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" also includes

computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "IT" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "IT" includes National Security Systems (NSS). (DoDD 4630.05)

Information Technology Architecture
An integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the Agency's strategic goals and information resources management goals. (DoDD 4630.05 and DoDI 4630.8)

Interoperability and Supportability Needs
A condition, situation, or capability in which interoperability and supportability deficiencies have been identified, based on an approved or established rule set, test, or measure of value for judging interoperability and supportability sufficiency of IT and NSS. (DoDD 4630.05)

Key Performance Parameters (KPPs)
Those minimum attributes or characteristics considered most essential for an effective military capability. KPPs are validated by the Chairman of the Joint Chiefs of Staff. (DoDD 4630.05)

Mission Partners
Those with whom the Department of Defense cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; state and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector. (DoDD 8000.01)

National Security System (NSS)
Any telecommunications or information system operated by the United States Government, the function, operation, or use of which

- Involves intelligence activities
- Involves cryptologic activities related to national security
- Involves command and control of military forces.
- Involves equipment that is an integral part of a weapon or weapons system.
- Is critical to the direct fulfillment of military or intelligence missions. This does not include automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance logistics, and personnel management applications). (DoDD 4630.05)

Net-Ready
The continuous ability to interface and interoperate to achieve operationally secure exchanges of information in conformance with enterprise constraints. The NR-KPP assesses the net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. (DoDD 4630.05)

Net-Ready Key Performance Parameter (NR-KPP)
The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. The NR-KPP is comprised of the following elements:

- Compliance with the NCOW RM.
- Compliance with applicable GIG Key Interface Profiles.
- Verification of compliance with DoD information assurance requirements.
- Supporting integrated architecture products required to assess information exchange and use for a given capability. (DoDD 4630.05)

Non-Materiel Solution
Changes in doctrine, organization, training, leadership and education, personnel, or facilities that satisfy identified capability gaps. (DoDD 4630.05)

Ontology
Formal representation of a domain.

Semantic
Of or relating to meaning, especially in language.

Standards Compliance
Confirmation that IT and NSS has undergone standards testing and exhibits a specified degree of standards conformity. (DoDI 4630.8)

Standards Conformance Certification
Confirmation by the DISA that an IT and NSS has undergone IT standards testing and exhibits IT standards-based implementation. IT standards include standards for information processing, information content (such as standard data definitions), information formats, and information transfer. (4630.8)

Supportability
The ability of systems and infrastructure components, external to IT or NSS, to achieve, aid, protect, complement, or sustain design, development, testing, training, or operations of the IT or NSS to its required capability. (DoDD 4630.05)

Syntax
The rules governing construction of software.

System Standards Profile
A system-specific list of all technical standards and guidelines for their use. To meet IT and NSS interoperability needs, the system standards profile should be built from applicable standards drawn from the DISR. (DoDI 4630.8)

Test and Evaluation
The act of generating data during the research and development of emerging systems and the creation of information through analysis that is useful to technical personnel and decision-makers for reducing design and acquisition risks. The process that gauges progress by measuring systems against requirements and specifications and analyzing the results. (DoDI 4630.8)

Unique Identification (UID)
A system of establishing globally ubiquitous unique identifiers within the Department of Defense, which serves to distinguish a discrete entity or relationship from other like and unlike entities or relationships. (DoDD 8320.03)

Unique Identifier
A character string, number, or sequence of bits assigned to a discrete entity or its associated attribute which serves to uniquely distinguish it from other like and unlike entities. Each unique identifier has only one occurrence within its defined scope of use. (DoDD 8320.03)

Appendix C - Standards Pros and Cons

The rating values are:

0 = cons to meeting criteria were judged to be more significant than pros

1 = pros to meeting criteria were judged to be more significant than cons

Category	Standards	Pros	Cons	Rating	Criteria	Source of Criteria
Vocabularies an terminology						
	DoD Doctrine(e.g. JP-02)	comprehensive; authoritative; common to DoD	may have to be interpreted	1	Does the standard allow the vocabulary to encompass enterprise terminology needed for interoperability across appropriate domains?	DoD Net Centric Data strategy May 2003; DoD IEA(enterprise priorities); AR 25-1(sec. 3.4, n)
	MDR	authoritative; common to DoD	have to look in other documents for vocabularies; more of an authoritative data source than a vocabulary standard	0	Does the standard require the terms in the vocabulary to be unambiguously defined?	DoD Net Centric Data strategy May 2003; DoD IEA(enterprise priorities)
	DISR	authoritative; common to DoD	no enforcement to enter standards	0	Does the standard require the vocabulary to be based on authoritative information(e.g. doctrine)?	AR 25-1(sec. 5.2,b)
	Mission area lexicons	authoritative: can be used to determine common teminology	Common to a COI versus among COIs	1	Does the standard promote commonality among vocabularies of systems that need to interoperate with one another?	Ar 25-1
	Enterprise identifiers				Can the standard be used to help measure the level of interoperability?	DoD IEA
	Open Technical Dictionary-Army 25-1		logical			
	DDMS	authoritative		1		

Category	Standards	Pros	Cons	Rating	Criteria	Source of Criteria
Data Models and Ontologies						
	DoDAF Meta Model (DM2)-conceptual, logical models	Extensible, can be used by many domains, well documented, flexibility to accommodate coomercial and other standards		1	Does the standard allow the model to contain an acceptable(to an appropriate authoritative body) set of data and relationships in the domain?	DoDAF 2.0
	OWL ontology modeling standard	Used to create DoD ontologies; widely used; Goes beyond basics semantics of RDF to express meaning of terminology in Web documents		1	Does the standard require the model to be extensible and accommodate relationships among domains?	World Wide Web Consortium
	UML – unified modeling languages(OMG standard)	used in commercial world; can be used to create DoDAF data models(e.g. Enterprise Architect)		1	Does the standard allow the model to leverage other open, commercial, and government standards?	World Wide Web Consortium
	ODMG object model-object data management group	Used to define objects	mainly used for storage not for semantic interoperability	1	Does the standard require the model to be maintained, documented, and used for interoperability certification and validation?	DoDAF 2.0
	RDF	general standard for expressing subject-predicate-object relationships;W3C standard for Semantic Web; RDF resources have unique identifiers	may be too general for determining commonality	1	Does the standard allow the model to be used as part of an overarching container model such as UCORE and/or NIEM?	DoD 8320.02
	XBRL	used mainly to express business information; can show relationships; is extensible		1	Can the standard be used to help measure the level of interoperability?	

Category	Standards	Pros	Cons	Rating	Criteria	Source of Criteria
Architectures						
	DoDAF	developed to help model the DoD mission areas; contains data and information views		1	Does the standard require the architecture to capture both the semantic and syntactic elements of IT interoperability?	DoD AF 2.0, Army AIA
	DoD IEA	provides policy and process guidance for data and services in a netcentric environment	does not contain technical standards	1	Does the standard allow the architecture be used to design, test, and evaluate activities that measure the degree of interoperability between IT systems?	DoDAF 2.0
	AR 25-1	Contains guidance to adopt enterprise identifiers(EIDs) ,industry standards including use of Open Technical Dictionary(OTD), and other industry standards as ISO standards for data quality management	only gives examples of standards to be used; no guidance on measurement of data commonality	1	Does the standard require that the architecture be documented and considered to be (by an appropriate COI) extensible for future changes?	DoDAF 2.0
	AIA	Contains guidance and standards for information exchange; contains some guidance for achieving semantic interoperability	no guidance on measurement of data commonality	1	Does the standards allow the architecture be used to help measure the degree of IT interoperability(as defined in CJCSI 3170) among IT systems?	CJCSI 3170
	GIG technical guidance(GTG);GIG Enterprise Service Profiles (GESPs)	A DoD authoritative configuration managed source of technical interoperability standards implementation guidance		1	Can the standard be used to help measure the level of interoperability?	DoDAF 2.

Category	Standards	Pros	Cons	Rating	Criteria	Source of Criteria
Repeatable Processes						
	DOD draft Business Operations Technical transition Plan - DCMO; OASIS - Web Services Business Process Execution Language (WS-BPEL) is an execution language o describe the behavior of end-to-end business processes	An example of a class of tools used to describe business processes; based on using XML	yet to be demonstrated for Warfighter IT	1	Does the standard require the process to be repeatable?	Army C2 Core Data Pilot
	RDECOM "Semantics First"	Can start with bottom up(Warfighter) or top down(doctrine) vocabularies; suggests developer/user interactions start early in process	not yet a standard-demonstarted in Army C2 Core data sharing pilot	1	Does the standards require the process to save time and effort compared to existing ways of accomplishing IT interoperability?	Sec. Army Sept. 2011 guidance memo
	Capability Maturity Model	Used to measure software development	not specific to measure common data	0	Can the standard be used to help measure the level of interoperability?	DoDAF 2
	Warfighter planning process	Used and understoodby Warfighters; based on criteria	not specific to measure common data	1		

Category	Standards	Pros	Cons	Rating	Criteria	Source of Criteria
Authoritative Data Sources including repositories						
	Meta Data registry	authoritative; common to DoD;		1	Does the standard require that an authoritative body has certified the data is the official source for a particular kind of information?	DoD IEA
	DISR	authoritative; common to DoD	contains references to data sources	1	Does the standard require that the ADS is a single source for that type of data?	Army AIA
	DTIC	authoritative; common to DoD		1	Does the standard require that the ADS reliable and trustworthy?	DoD IEA
	CADIE	authoritative; common to Army		1	Does the standard require that the data are being maintained in accordance with policies and procedures that govern authoritative data sources (ADSs)?	DoD IEA
	DARS	authoritative; common to DoD	contains references to data sources	1	Does the standard require that the repository be accessible in near real time?	DoD Netcentric Data Strategy 2003
					Does the standard require that data in a repository be found within a acceptable amount of time to most users?	
					Can the standard be used to help measure the level of interoperability?	

Appendix D - Data Call Responses

COE IT Programs

Command Post Programs	Data Call Response
Distributed Common Ground Station – Army CPD (DCGS-A)	x
Command Post of the Future (CPOF)CPD	
Global Command and Control System – Army (GCCS-A) CPD	
Advanced Field Artillery Tactical Data System (AFATDS) CDD	
Battle Command Sustainment and Support System (BCS3) CPD	
Air And Missile Defense Work Station (AMDWS)	
Joint Warning and Reporting System CPD	
Tactical Airspace Integration System CPD	x
Integrated Base Defense ONS	
Aviation Mission Planning System (AMPS) ORD	x
Joint Battle Command – Platform (JBC-P), CDD	
Maneuver Control System (MCS), CPD	
Warfighter Information Network – Tactical (WIN-T), CDD	
Battle Command On The Move (MBCOTM), CPD	

Mounted Programs	Data Call Response
JBC-P Joint Battle Command-Platform (JBC-P)	x
FBCB2 Joint Capabilities Release (JCR)	
FBCB2 Movement Tracking System (MTS) JCR-Log	x
FBCB2 Tactical Ground Reporting System (TIGR) Began FY11	x
MC FSC2 Forward Observer System (FOS) and/or Effects Management Tool (EMT)	
MC FSC2 Advanced Field Artillery Tactical Data System (AFATDS)	
TMC Command Post of the Future (CPOF) Begin FY12	
WIN-T NETOPS	

Data Center / Cloud Programs	Data Call Response
Acquisition Business (AcqBusiness) Acquisition Business (AcqBiz) Central Portal	
Acquisition, Logistics and Technology Enterprise Systems and Services ALTESS Data Center	
Army Enterprise Systems Integration Program (AESIP)	
Army Human Resource System (AHRS)	
Army Knowledge Online (AKO)	x
Enterprise Directory Service-Lite (EDS-Lite)	
Computer Information	
Hardware, Enterprise Software, and Solutions (CHESS)	x
Defense Messaging System-Army (DMS-A)	
Tactical Message System (TMS)	
Department of Defense (DoD) Biometrics, Biometrics Enabling Capability (BEC)	x
DoD Biometrics, Tactical Biometrics System	
Distributed Learning System (DLS)	x
Army Learning Management System (ALMS)	
Force Management System (FMS)	
General Fund Enterprise Business System (GFEBS)	x
Global Combat Support System—Army (GCSS-Army)	x
Human Resource (HR) Solutions	
Installation Management Systems—Army (IMS-A)	
Range Facility Management Support System (RFMSS)	
Integrated Personnel and Pay—Army (IPPS-A)	
Joint-Automatic Identification Technology (J-AIT)	x
Logistics Modernization Program (LMP)	x
Medical Communications for Combat Casualty Care (MC4) (**See Mounted CE)**	x
Reserve Component Automation Systems (RCAS)	x
Transportation Information Systems (TIS)	
Automated Air Load Planning System (AALPS)	
Automated Movement Flow Tracking In-Transit Visibility (AMFT-ITV)	
Air Movement Request (AMR)	
NIPRNet Globe Services (NGS)	
Transportation Coordinators Automated Information for Movements System II (TC-AIMS II)	
TIS Enterprise	
TC AIMS II	x
Global Mission network (OGE)	x

Mobile Handheld Programs	Data Call Response
PEO Ammo Lightweight Handheld Mortar Ballistic Computer	x
PEO C3T Forward Entry Devices	
PEO C3T Gun Display Unit-Replacement	
PEO C3T Joint Battle Command-Platform (Handheld)	
PEO C3T Lightweight Tactical Fire Direction System Centaur	
PEO C3T Mobile Handheld Simple Key Loader SKL	

PEO C3T Common Hardware System	
PEO EIS Joint Personnel Identification, Version 2	x
PEO EIS Medical Communications for Combat Casualty Care	x
PEO EIS Property Book Unit Supply Enhanced	
PEO IEW&S Army Counterintelligence and Human Intelligence Automated Reporting and Collection System	
PEO IEW&S Machine Foreign Language Translation	x
PEO IEW&S Modernized Global Positioning User Equipment	
PEO IEW&S NAVSTAR Global Positioning System	
PEO IEW&S Tool Set, Technical, Engineering, Engineer Field Planning, Reconnaissance, Surveying, and Sketching Set	
PEO Soldier Nett Warrior	
ENFIRE	x

RT Safety Program	Data Call Response
OH-58D and OH-58F Scout Attack Helicopters.	x

JAMD Data Call Response

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
		Joint Air and Missile Defense system	Joint Integrated Air and Missile Defense	JDES IPT JIAMD Logic Data Models; Common IAMD XML Schema (CIXS); DoD MLSTDs (USMTF, Link-16, VMF); BMDS XML Standard (BXS); Global Sensor Integration on Networks (GSIN)	Common IAMD XML Schema (CIXS)	JAMD COI Vocabulary v1.0; USSTRATCOM GMD Lexicon	Standing doctrine, concept of operations, and TTPs were considering in the development of the JIAMD Logical Data Models	Established a COI; Adopted the STRATCOM GMD Lexicon	The JAMD COI has established a Common IAMD XML Schema (CIXS) Configuration Control Board (CCB) comprised of Programs of Record within the JAMD community and operating under the oversight of the JAMD COI with governance from the Protection Functional Capability Board (FCB).

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
No	Systems currently validate and certify the interoperability of their interfaces with the connecting systems as part of their individual program baselines.	Use of a common data set consistent with the JAMD Vocabulary ensures semantic interoperability.	Approximately 10 months of community effort to initially develop the CIXS; CIXS CCB meetings are now scheduled monthly.				Yes. The CIXS CCB has an approved charter and established procedures to address submission of changes, the voting process, and an appeals process.

RT Safety Data Call Response

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
RT Safety		OH-58D and OH-58F Scout Attack Helicopters				VICTORY - VICTORY is an architecture and standard set of specifications that facilitate interoperability and reduced platform SWaP; FACETM – FACETM establishes a standard common operating environment to support portable capability applications across Department of Defense (DoD) avionics systems.; OIS - OIS establishes a standard common interface across Munitions Systems, Munitions Control and Guided Tube Launched Munitions Fuze Setters.			

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
	I2E and AIC test events. All testing is supporting from our Aviation SIL located at the Software Engineering Directorate (SED) at Redstone Arsenal, Alabama.				We interoperate with other systems via VMF messages over the BFT network.		

Command Post Data Call Response

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
Command Post	Mission Command	AFATDS*, AMDWS, AMPS, BCCS (Includes Infrastructure Services)*, BCS3*,Command Web*, DCGS-A (Client), DCGS-A (Server), GCCS-A*, JADOCS*, JEM, JWARN, Mission Command Workstation (MCWS)*, STAMIS Capabilities (Selected), TAIS		Mission command systems and capabilities implement a number of a data models on the host systems of the respective program. These data models are influenced by a number of the existing data models (JC3IEDM, UCORE) and interoperability standards (USMTF, VMF, MC DDS Schema, MIP, etc). Note that MC systems do not fully implement any of the current data models in their entirety on their systems.	There has not been a comprehensive implementation of the above data models to date. Programs currently implement capabilities and the supporting data models to satisfy the requirements of the respective TCM or user.	Many of the common attributes of the data models inform the data dictionaries of the MC systems. Common attributes on how time, coordinates, attributes of USMTF and VMF messages, and XML schemas inform the data dictionaries of the individual systems. Recently developed systems may or may not have metadata repositories to further describe data.	MC and CP CE systems span each of the WFA's of mission command, protection, sustainment, fires, intelligence, and movement and maneuver. There are a large number of Army and Joint Publications that inform the vocabulary of the respective systems beginning with JP 3-0 and ADP 3-0 and extending into the full range of JPs, FMs, ATTPs, TCs, and other supporting publications	MC systems support a number of COIs related to the Joint Command and Control Efforts as well as the Air Operations COI.	MC has a current System Engineering Plan that describing the configuration management process.

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
Currently MC systems undergo a range of Factory Acceptance Testing, Government Confidence Testing, Army Interoperability Certification, and other safety, joint, developmental, and operational testing as directed by the program.	No specific data model was explicitly used.	Semantic interoperability is currently limited to the ability of current interfaces to exchange data. The most common ways that are currently used within MC are Web Services (generally point to point), VMF, USMTF	The time would be dependent on the specific program and the level of maturity of the program.	No system or system of systems currently uses a fully unified data model within the Army, Service Components, Joint Systems, and multinational partners. Interoperability is currently achieved via document message standards and point to point services			The request would be dependent on the specific program.

Mounted Data Call Response

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
Mounted		MTS (JCR LOG)	Joint Capabilities	No data model	No				
		TIGR	Warfighting Mission Area, Joint Capabilities	ASCOPE - TIGR data model is reflected in its physical database schema	No				
		JBC-P	Warfighting Mission Area, Joint (Army PMO)	DCAT Model	Yes	PM Mission CMD DDS, MIL STD 2525B, TIGR, MDL, MIL STD 6017A	JBCP CDD	Data Mgmt Interop Group, VMF Stds Group	Yes

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
					VMF messaging		
					Binary Transfer of Database Tables		
Yes	Yes	Use defined standards, CTSF, JITC	Unknown	Not particularly applicable			Yes

Data Center Data Call Response (Page 1)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
	EIS	Logistics Modernization Program (non-POR)	Business Mission Area with emphasis in Logistics and Army Working Capital Fund	Conceptual, Logical and physical	LMP product Management Office has initiated steps to add Department of Defense Architecture Framework (D0DAF)				
		CHESS IT E-mart website	The buying of commercial IT by the Army, other DoD Agencies and the Federal Government through the Smart BUY program	The data model is consistent with displaying and capturing information from the website and in capturing the sales from the vendors that have contracts/agreements with CHESS	None				
		Distributed Learning System (DLS) POR	G-1 Training	DLS used conceptual, logical, and physical data models to help design, develop and test the system	Semantic modeling was not a program requirement				

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
LMP is working with the Office of Business Transformation on the DoD-wide Semantic Web initiative in terms of data compliance with the release of the Business Enterprise Architecture within release v9.0.							
					The CHESS IT E-mart does not exchange any information with other systems at this time		
		There was no requirement to validate and certify semantic interoperability			The DLS program exchanges data with the Army Training Requirements and Resources System. DLS uses XML Message to exchange data. A data dictionary was used to designate the fields of data for exchange		

Data Center Data Call Response (Page 2)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
		General Fund Enterprise Business System (GFEBS)	GFEBS is a financial system in the Business Mission Area. GFEBS supports financial management and acquisition	GFEBS created and maintains the DIV-1: GFEBS Top-Level Conceptual Data Model, DIV-2: GFEBS Top-Level Logical Data Model and DIV-3: GFEBS Top-Level Physical Data Model	OSD(I&E) directed that GFEBS develop a data dictionary to show alignment with the Real Property Information Model (RPIM). GFEBS has additionally developed a Data Dictionary based on the DCMO's SFIS compliance checklist to show compliance with SFIS standards and business rules. GFEBS maintains a detailed Requirements Traceability Matrix (RTM) that details the source documentation of GFEBS system designs, vocabularies, and functionalities	The Standard Financial Information Structure (SFIS) and the Real Property Information Model (RPIM) are the enterprise data standardization initiatives applicable to GFEBS' scope and the bounds of the logical and physical data models developed and maintained by the program	The Capability Production Document (CPD) for the General Fund Enterprise Business System (GFEBS) provides the functional requirements for GFEBS. This document is based on requirements from the Chief Financial Officers Act, the Defense Finance and Accounting Service (DFAS) Guide to Federal Requirements for Financial Management Systems, the Federal Financial Management Improvement Act, the Government Management Reform Act and other laws and regulations	Interface Partner Working Groups have been conducted with interface partners to establish agreed upon vocabularies and other interface requirements	The ARIS architecture tool internally records modification dates as artifacts are updated. The ISP process determines the baseline architecture

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
The BEA requires the use of the ACART tool to assert compliance with the latest (annual) version of the BEA. The SFIS team from DCMO in 2011 conducted an audit of compliance to SFIS data standards and business rules. Artifacts (data dictionary, table layouts, real property data) have been submitted for review for RIPM compliance	The SV-6 was submitted both to ATEC and JITC to support interoperability evaluations. Semantic interoperability was verified during IOT&E in 2009 and the follow-on LUT in 2010	Semantic interoperability has been certified by JITC on GFEBS' operational interoperability with the interface partner systems	Approximately 3 to 4 man years	The interoperability environment is typically not stable due to the frequency and unanticipated consequences of requirements changes. Certification processes are often geared to simpler standalone legacy systems and are not geared to the complexity of development and testing required in ERP system implementations. Annual changes to compliance requirements are challenging for ERP systems to implement rapidly due to large data sets, more stringent testing requirements, cost, etc. Policies are needed that recognize the unique demands of larger-scale ERP implementations	GFEBS has also registered its web services' operational end points in the DoD MetaData Registry and the Net-Centric Enterprise Services Universal Description Discovery and Integration Registry (NCES UDDI). The GFEBS identifier is um:US:USGovt:Army:USANORTH:GFEBS. The MDR Namespace is DOAGFEBS, the NCES UDDI Namespace is US USGovt Army USARNORTH GFEBS. At this time, three services are listed: FunctionalLocationSearch, NotificationCreate, NotificationStatus which provide information		

Data Center Data Call Response (Page 3)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
		ABIS(QRC)	Battlespace Awareness, Force Application, Logistics, Command and Control. Netcentric	None					
		BEC		None					
		JPIv2		None					
		BISA		None					
		BAT4.0(QRC)		None					
		BAT5.0(QRC)		None					
		AKO	Enterprise Information Environment Mission Area	Logical and physical	Semantics for data used came from authoritative source. All AKO data input into IdM comes from DoD HR sources. We use the HR source semantics				

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models

Data Center Data Call Response (Page 4)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
		RCAS	Force Management, Force preparation, Human Capital Management, Netcentric, Information Assurance, Protect Data and networks	RCAS has utilized logical models and physical data models	Yes, RCAS is now in sustainment and physical data models are automated and updated by release. Current RCAS Data Dictionary supports Release 6.1.12.12	DoD Data Dictionary standards	Concept of Operations	Integrated process teams (IPT)	the PDRCAS Configuration Management Plan (CMP) covers all documentation generated by the PD and the Prime Integrator and is maintained in the Government CM Library

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
The PDRCAS employs rigorous joint testing and IA scanning utilizing both manual and automated test tools such as Quick Test Pro and Load Runner for testing and the requisite IA Scanning tools such as Production Gold Disk, Oracle SRR Scripts and Retina to ensure IA Compliance	the test scripts are developed and updated with every release using the latest data models to ensure any changes to the Interface Exchanges are captured and tested during the various test phases	Development testing and formal testing	Initial data models were created by a dedicated Database Design team that varied between 2 and 6 FTEs per year over a 20 year period	Clear and high level standards, requirements and examples back at program initiation over 24 years ago (1988 was requirement gathering)		The Reserve Component Automation System (RCAS) is a scalable, open-systems environment, automated information system that supports commanders with information needed for Reserve Component mobilization and day-to-day administrative operations	A link to the RCAS data models is on the RCAS Home page on AKO. (https://www.us.army.mil/suite/page/207093)

Data Center Data Call Response (Page 5)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
		Global Mission Network (OGE)	Connectivity, Voice over Internet Protocol (VoIP), Email and Chat hosting Virtual/Enclave Hosting, Distance Replication vi) Battle Command and Control Systems (BCCS) hosting vii) Battle Command Enterprise Systems (CPOF) viii) NETOPS	OP VAL One and Two (Physical/Logical),b) Replications Tests (Physical/Logical),Virtual Environment interoperability tests (Physical/Logical), Architecture and Engineering overlap discussions (Conceptual/Logical)			Operational Views, System Views, Concept of Operations (ConOps), Best Practices for logical separation of data	Working Integrated Product Teams (WIPT), Integrated Product Teams (IPT), Working Groups, Sharepoint Collaboration tools , Engineering Integration Sessions, Engineering White Boarding Sessions	our Configuration Manager oversees this process and sits on several Change Control Boards

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
we are in compliance with all DoD/Army Regulations	some tests of distance replication and virtual integration were undertaken to verify that the OGE systems were operationally compatible with forward TCFs	Operational tests and transfer tests. Used the systems to undertake designed actions with test systems and verified operation at destination. Metrics and other measurements were taken over the course of the tests; Our system backbone is primarily secure transport (Black Core) and all data is encrypted at both ends thus our focus was how does encrypted data traverse the transport and how does it interact with other mission systems. Validation occurred when other DoD Agencies requested use of our secure transport to support their growing bandwidth requirements	Approximately two (2) man years to engineer, test and validate. (If you include Op Val 1 and 2 as well as Block 1 then it is whole teams for over 2 years including P2E, Vern was old lead)	Gaining buy-in from the Information Assurance community of interest, Greater Engineering Integration across Army Entities and Theaters	Yes		Yes, they are kept on the PM P2E portal

Data Center Data Call Response (Page 6)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
		RF-ITV	The Radio Frequency In-transit Visibility (RF-ITV) capability supports the 'LOGISTICS' Joint Capability Area (JCA)	We used the DoD Architecture Framework (DoDAF) version 1.5 during system development and testing. This capability was a prototype system that went live in 2003. We took a semi-mature capability and built around the already developed logical data models, or Operational View 7 (OV-7), and transposed that into a robust physical data model, or System View 11 (SV-11), as system development matured. Our Sustainment strategy includes developing DoDAF 2.0 compliant architecture products when improvements are made	We have a database dictionary that provides detailed descriptions of every data element in our database. For each data element we provide the element's name, definition, type and length, and table in which it appears. The document also provides the definitions and Structured Query Language (SQL) descriptions of each table. Next to each table's name is its primary key (single element or multi-element (composite)) if it has one. Below each table's name is its definition and list of columns described by three attributes: the name, whether a null value is and the data type and length	Much of our metadata (service offerings) is registered and defined in the DoD Metadata Registry and resides in the Transportation Community of Interest (COI)	There are many starting with a Mission Needs Statement (MNS), Operational Requirement Document (ORD), Logistics Automatic Identification Technology (AIT) Concept of Operations (CONOPS), numerous Combatant Commander (CCDR) Messages, DoD Radio Frequency Identification (RFID) policy, and DoD Automatic Identification Technology (AIT) Concept of Operations (CONOPS)	We are members of a Joint forum that meets weekly to discuss everything related to the global use of Radio Frequency Identification devices and the missions the technology supports	Yes, nothing in our database changes without being voted on by a fully qualified engineering review board (ERB). After the ERB approves a change a structured Configuration Management process is followed to develop, test, and accept any changes

Data Center Data Call Response (Page 6 continued)

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
The data models are integrated into our DoDAF model. Our system architecture was tested and certified by the Army	Many, if not all of our DoD Architecture Framework models were provided to the Joint Interoperability Test Command (JITC) to support our interoperability and supportability certification	Formal testing is conducted before any interface is released into the production environment	Approximately 150 man-hours consumed per new interface. Semantic interoperability is accomplished through open lines of communication during the development of data exchanges with our interface partner. We can provide them with our data dictionary, XML Schema Definition (XSD), or Web Services Description Language (WSDL) documents that thoroughly describe our metadata. These documents can also be discovered in the DoD Metadata Registry. Additionally, we create an Interface.Control Documents (ICD) that clearly documents what and how data is to be exchanged. I am unable to provide a number of man-years that it took to develop models for initial testing			RF-ITV is a mission essential information system that supports Joint operations. RF-ITV uses Radio Frequency Identification (RFID) devices to support the dissemination of In-Transit Visibility (ITV) information required by the Department of Defense (DoD), Coalition Partners, and Allies of the United States. By using RFID tags on shipments of supplies equipment, the RF-ITV system traces the identity, status, and location of cargo from origin (depot or vendor) to destination	Yes

Data Center Data Call Response (Page 7)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
		GCSS-Army		OAGIS and SAP		OAGIS	Focused Logistics	Logistics COI under the G-4	GCSS-Army's lead architect is responsible for all DoDAF products. The DoDAF products are developed using IBM Rational System Architect. This tool internally records modification dates as artifacts are updated
		TC-AIMS II	Deployment and Distribution – Unit Movement Planning	Generated from a logical model to a physical model via ERWIN	None	TRDM (formerly TMDS), SDDCTEA TB -55, TC-AIMS II data dictionary	Defense Transportation Regulations, Integrated Database Design Document, CONOPS	DPMO Configuration Control Board, Fort Lee, VA	DPMO Configuration Control Board, Fort Lee, VA

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
GCSS-Army is built using commercial-off-the-shelf (COTS) software, SAP. This software has an inherent taxonomy and ontology utilizing commercial best business practice standards	Yes	During the development of SAP, the data model and related business processes go through rigorous software development testing. In addition to this testing, GCSS-Army utilizes standard DoD developmental and operational software testing practices including interface testing, commercially referred to as trading partner testing, during this testing, the commercial standard and custom enhancement developed XSDs are used as the standard for testing	3 man years	If the DoD would adopt a standard for enterprise resource planning systems data models, the industry would then build to that standard. An example of this would be MIMOSA for the auto industry			Only at the edge of the system, i.e. interoperability data models
Government Acceptance Testing	SV-6 Systems/Services Data Exchange Matrix, OV-2 Operational Node Connectivity Description, TV-1 Technical Standards Profile	JITC; Interface testing against IDD with external systems during Government Acceptance Testing And JITC	Unknown	If all interfaces had to validate their data models and business rules through Schemetron on the DDMS site	Additional data added through Interface Description Documents and MOA		DISR Online, ERWIN models in CM

Mobile Handheld Data Call Response (Page 1)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
Mobile Handheld		Joint Personnel Identification System version 2 (JPIv2)	Net-centric, Information Transport (IT), Enterprise Services (ES), Net Management, Information Assurance, Battlespace Awareness	None yet		Applicable DISR standards and GTPs			
		Biometric Automated Toolset – Army (BAT-A)		None					
		Instrument Set, Reconnaissance, and Surveying (ENFIRE)	Command and Control	DoDAF		UML	Doctrine, CONOPS	Working Groups, technical exchange meetings	Yes

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
					No systematic analysis was ever performed to generate data exchange methodologies or standards for any of the tactical biometric systems deployed to date. In order to satisfy existing interoperability requirements with other systems, e.g. the Distributed Common Ground System – Army (DCGS-A), an abstraction layer or Application Programming Interface (API) was developed starting in early 2009	JPIv2 provides the joint solution to biometrics collection and analysis for Department of Defense. The capability is intended to support identity dominance across the full spectrum of operations for all services. The capability will be used in two major variants, a portable version for use in the field and a mobile version for forward garrison use. Fielding expected FY14	
		Completed in late 2011, the BAT API, consisting of a framework and exposed web services, remains to be tested with the DCGS-A Ozone Framework and Widgets prior to deployment					
ENFIRE laboratory test threads	Off-Site integration testing	Army Central Technical Support Facility					Yes

Mobile Handheld Data Call Response (Page 2)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
		Lightweight Handheld Mortar Ballistic Computer (M32)	Indirect Fire Support	OV's TVs'		MIL STD 6017 to exchange data between other systems			
		Machine Foreign Language Translation System (MFLTS)	Base Physical Security	None yet		Applicable DISR standards and GTPs; an open API will be developed for host platforms to interface to the MFLTS application			
	EIS	Defense Health Information Management System (DHIMS); AHLTA-Mobile Information System	Joint Logistics, Force Health Protection, and Joint Battlespace Awareness – Situational Awareness	Electronic Health Record (EHR) and Medical Command and Control (C2) and uses logical data models	Established semantics and terminologies are in use as determined by the MHS, VHA and international standards bodies	Subset of Health Level Seven (HL7) International	AHLTA-Mobile CONOPS	Technical Interchange Meetings (TIM) with Defense & Veterans Brain Injury Center (DVBIC), Department of Defense (DOD), Medical Communications for Combat Casualty Care (MC4)	DHIMS Configuration Management Standard Operating Procedures (SOP)

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
		Engineering and Formal Testing in our Labs, plus testing at CTSF which results in an AIC			Standard Fire Support Terminology used and MIL STD 6017 standards used		
						We are developing a Machine Foreign Language Translation System (MFLTS) capability for the U.S. Army which will be a software only application capable of doing both two way speech-to-speech and two way text-to-text language translation	
DISA Security Technical Information Guide (STIG)	Yes	Systems Integration Test - JMIS DT&E, end-to-end testing is completed to obtain a JITC accreditation as part of the PEO EIS Authority to Operate (ATO)	No metrics available	Better requirements model	Interface Control Document (ICD), Database Design Document (DBDD)		

Sensor CE Data Call Response (Page 1)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
Sensors	IEW&S	Distributed Common Ground System (DCGS-A)	JCA 2.0 Battlespace Awareness and JCA 5.0 Command and Control	The Joint DCGS Metadata Framework registered on the MetaData Repository (MDR)		DDMS 2.0 as part of the Joint DCGS Integration Backbone (DIB)	Organization doctrine is driven by Joint Publication 2.0 and Field Manual 2.0 Intelligence and other related Army Field Manuals	DCGS-A participates in the Joint DCGS Community MetaData Management Team (MMT) that is part of the Joint DCGS Management Office (DMO)	Standard PM DCGS-A configuration management process is following within the Army and then overall CM of Joint Data Model by Joint DCGS DMO

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
The Joint DCGS community is looking into the use of ConTesa as a test tool for the DCGS DIB MetaData Framework and associated schemas	The DIB is essential for Discovery and receipt of metadata and associated data from other DCGS systems. Previously used the Empire Challenge demonstrations in a Joint and Coalition environment. A new Enterprise testing event is anticipated in the future		PM DCGS-A direct labor to data models and semantic interoperability are approximately 10 man-years per year between PM office SETA and actual vendor work	Reduce the number of un-necessary redundant standards. Current Army Data standardization problem is to normalize and harmonize Mission Command, Logistics and Business and Intelligence Community metadata and data			

Sensor CE Data Call Response (Page 2)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
	IEW&S	Counterintelligence and Human Intelligence Automated Reporting and Collection System (CHARCS)	Battlespace Awareness, Force Application, Command and Control, Net-Centric	Logical (Military Occupational Specialty (MOS) Critical Task Lists)	Vocabularies and terminology used were derived directly from existing Army doctrine	None			
	IEW&S	Computer, meteorological data – Profiler (cmd-p) program of record		None		MIL-STD-6017B			
	IEW&S	DAS-2		None					
	IEW&S	LYNX I/II							

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
	Validation and interoperability testing occurred at the Central Technical Support Facility at Fort Hood TX					PD CHARCS develops deployable automated information management systems to provide near real time collection and dissemination of Counterintelligence and Human Intelligence via a comprehensive software application and through the use of a number of CI/HUMINT tools and supporting kits that provide numerous capabilities for collection such as voice recording, photography under day or night conditions, as well as exploitation of digital and cellular media	
	EXCHANGED FIVE JVMF MET MESSAGES WITH AFATDS; DAU TEST SEQUENCE PROCESS -> FQT, DT, AIC, LUT						
						QRC Afghanistan	
						QRC Afghanistan	

Sensor CE Data Call Response (Page 3)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
	IEW&S	Persistent Threat Detection System (PTDS)	OEF Mission providing Intelligence, Surveillance, Reconnaissance (ISR), and Force Protection (FP) capabilities. Sensor data is disseminated among various tactical units within the battlespace		CONOPS, SV-1 drawings, Systems Engineering Plan (SEP), Configuration Management Plan (CMP), SV-1 drawings; Glossary-terms in supporting documents for the overall system. Lexicons in software models			None	Yes
	PEO C3T	ABCS							
	Army Corps of Engineers	AGC							
		UH-60M	3.1.2.3 Land(MTI); 4.1.1.2 Operationally Move the Force;4.1.2 Sustain the Force;4.1.2.1 Deliver Non-Unit-Related Cargo;4.1.2.2 Deliver Non-Unit-Related Personnel	DADIF?	The UH-60M software uses verbiage from Military Standards for its terminology	VMF (MIL-STD-6017)			

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
DoD Information Assurance and Accreditation Process (DIACAP)	Integration testing at Yuma Proving Ground			Concurrently establishing Memorandum of Agreements (MOAs) between all relative parties while testing, but prior to fielding		PTDS is an aerostat system providing an Ariel layer of communications	
	Software Integration Lab testing and AIC are used to validate and certify interoperability						

Sensor CE Data Call Response (Page 4)

Computing Environment	PEO	System	Mission Areas Supported	Data Model	Semantic Content	Standards Used	Source Documents for Data Models	Forums to Develop Vocabularies (e.g., COIs)	Configuration Management Process
	IEW&S	Machine Foreign Language Translation System (MFLTS)	MFLTS supports the Warfighter, Mission/Battle Command, the Intelligence Community (IC)	A MFLTS Data Collection IPT developed a format for collected language data, which included audio and text documents. Conceptual, logical and physical data models are being developed as part of the MFLTS Software Architecture and for some of the DoDAF Version 2.x Architecture Products		DISR Online is and will be used for software that is currently in the TD Phase; 1. GTG Federation System; 4. An outside agency (e.g. SPAWAR) expert in software development standards will review all standards that will be considered when developing the data dictionaries, metadata repositories or lexicons that support the data models	TTPs; CONOPS; Military Domains – specific procedures and related military jargon for each domain; MFLTS Software Architecture	Integrated Product Teams (IPTs) and Working Groups (WGs)	The development contractor employs a Software Configuration Control Board (SCCB) and the MFLTS Program Office has an SCCB. These processes are complimentary and support the CM process; documentation is being designed and put in place. The CM process will be baselined and fully in place by the end of the TD Phase

Testing for System Compliance with Data Models	Verify and Certify Interoperability Using Data Models	Process Used to Validate Interoperability	Time and Effort to Create Initial Data Models	Suggested improvements	Identification of Terminology	Description	Documented Data Models
				If there is not already one in place, perhaps a standard for all issues to be negotiated with host platforms supporting software applications for MOA development should be established for PEO IEW&S. The program office has and is developing MOAs with host platform systems outlining standardized issues. These MOAs are reviewed annually			

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
22-07-2012	Technical	11-08-2011 to 22-07-2012

4. TITLE AND SUBTITLE
Warfighter IT Interoperability Standards Study

5a. CONTRACT NUMBER
W15P7T-06-D-E401

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Bleach, Richard
Morosoff, Peter
Seeley, Jeff

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Electronic Mapping Systems, Inc. (dba E-MAPS)
10340 Democracy Lane, Suite 302
Fairfax, Virginia 22030
Email: e-maps@e-mapsys.com
Website: www.e-mapsys.com

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Army Chief Information Officer
(US Army CIO/G-6)
Architecture, Operations, Networks and Space Directorate
Information Architecture Division
Building 220, Fort Belvoir, VA 22060

10. SPONSOR/MONITOR'S ACRONYM(S)
US Army CIO/G-6

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report explains the findings and recommendations of the Warfighter Information Technology Interoperability Standards (WITIS) Study on the standards available to facilitate interoperability across the IT systems developed to support Warfighters. The study team found (1) there is no standard DoD definition of interoperability and (2) this leads to a variety of opinions as to whether interoperability is based on 1) just standards such as eXtensible Markup Language (XML) that address formatting but not semantics; 2) semantics (e.g., uniform understanding of the term fire support) and format (syntax); or 3) semantics and format plus relevant policy and procedures, registries, data architecture, and structures such as data models. The study team concluded that creating interoperability requires using the third set of elements (i.e., semantic, format [syntax], and policy and procedures). The biggest gap in creating semantic interoperability is insufficient Army and DoD policy and process on IT inter-operability. The study recommends that the IT interoperability gaps in Army and DOD policy and process be identified and closed. Additional actions should be taken to remedy shortcomings with registries and repositories, data architecture, and data models and ontology that impede IT interoperability.

15. SUBJECT TERMS
Data interoperability, warfighter interoperability, semantic, IT standards

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Jeff Seeley
Unclassified	Unclassified	Unclassified		108	19b. TELEPHONE NUMBER *(include area code)* 703-385-9320